UNIVERSITY OF NAIROBI

MOBILE BANKING SECURITY

Enhanced Mobile Banking Security: Implementing Transaction Authorization mechanism via USSD Push.

WYCLIFFE OCHIENG' AGWANYANJABA

P53/13191/2018

This research report is submitted to the School of Computing and Informatics in partial fulfillment of the requirements for the award of the degree of MSc Distributed Computing Technology of the University of Nairobi

DECLARATION

I Wycliffe Ochieng' assert that this research report is my original work and has not been presented for the award of a degree or for any other similar purpose in this or any other institution. To the best of my knowledge, this report contains no materials previously written or published except where due reference is made.

Signature: ……………………………. Date: …………………………

Wycliffe Ochieng'

P53/13191/2018

This research report has been submitted for examination with the approval of me as the supervisor

Signature: …………………………... Date: …………………………

Christine A Ronge

Lecturer, School of Computing and Informatics

University of Nairobi

ABSTRACT

Mobile initiated financial transactions need to be authenticated. This is a mandatory requirement since it serves as a security step or mechanism against non-repudiation. This is true for Mobile Banking customers in Kenya. The stage of protection for a given authentication scheme relies upon on characteristic combination, authentication channel, credential storage, and encryption. A range of researches had been performed on mobile banking authentication and their stage of protection. Research has proven challenges related to single factor or two factor authentication schemes. However, there are inadequate studies on authentication schemes that mixes different factors of authentications for secure and efficient mobile banking transactions.

The goal of the research was to explore challenges of using PIN as the only factor of authentication and further evaluate the effectiveness of incorporating a combined USSD push and PIN efficient multifactor authentication. Convenience non-probability method was used to identify a subset of the population and Snowball Sampling used to target a total of 385 respondents. A total number of 442 responses were received through online administered questionnaires. The study found 84.4% of the respondents use mobile banking frequently. That is to say, many times during the daily lives. Further finding was, the de-facto login method used in mobile banking applications in Kenya, is via PIN and 69% of respondents have incurred losses due to compromised PINs. These descriptive statistics necessitated a need for secure mobile banking app. Hence a need for multi factor authentication.

The solution implemented offers remedy to challenges faced by mobile banking customers in Kenya. This solution was not entirely user's PIN dependent but also tied to other details such as International Mobile Equipment Identity (IMEI), Mobile Systems International Subscriber Identity Number (MSISDN), and International Mobile Subscriber Identity (IMSI) in addition to time bound USSD push augmented with biometric authentication, Fingerprint. These attributes were encrypted using BCrypt Hashing Function in mobile banking applications. The storage of credentials was in distributed locations in encrypted format. The architecture employed provided improved security from cyber-attacks such as: identity theft, phishing, social engineering, spoofing and man in the middle attack.

In conclusion, use of USSD push in mobile banking provide an efficient layer of authentication hence improved mobile banking security.

Keywords: **Mobile Banking, Security, USSD, GSM, Authentication, Encryption, Cloud Computing, Cyber-Attacks**.

ACKNOWLEDGEMENT

Sincere gratitude to my supervisor Christine Ronge for her dedication. Thanks for your precious time and guidance that has enabled me successfully to complete this research work, I am forever grateful.

In a special way, I thank my mother, Caroline Mado for upright upbringing and installing confidence that has define the person aim today. Special thanks to my siblings: Vivian, Ruth, Paul and Kevin for their unwavering support during my undertaking of the research. I will forever be grateful.

LIST OF TABLES

LIST OF FIGURES

LIST OF ABREVIATIONS

AI-Artificial Intelligence
API – Application Programming Interface
USSD – Unstructured Supplementary service Data.
GSM – Global System for mobile communications
IMT – International Money Transfers
MNO – Mobile Network Operators
PIN – Personal Identification Number
MSISDN – Mobile Station International Subscriber Directory Number
M-PESA – Mobile payment service in Kenya offered by Safaricom PLC.
IMEI – International Mobile Equipment Identifier
IMSI-International Mobile Subscriber Identity
SMS – Short Messaging Service
SMSC – Short Message Service Center
MySQL- is an open-source relational database management system.
OWASP- Open Web Application Security Project
ISO/IEC- is a combined technical committee (ISO and IEC) whose mandate is to improve, preserve and promote standards in the fields of ICT.
REST-Representational State.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

1.1 BACKGROUND

In Kenya, the mobile subscriber base continues to grow. According to the Communications Authority of Kenya (CAK, 2019), the number of registered subscribers in the country has grown by 6.2 percent from the previous quarter to 49.5 million. Of these, the number of active mobile cash subscriptions stands at 31.6 million in 2019. This kind of growth poses a potential for huge transformation in financial sector in Kenya as financial institutions get alternative revenue streams by offering banking services via mobile channels. In a survey by Kenya Bankers Association (Ochieng & Watson , 2014), Mobile banking (m-banking) is defined as delivery and availing of banking services through telecommunication infrastructure by leveraging on mobile phones. The range of services provided may perhaps include conveniences to do all bank transactions, manage accounts in addition to access personalized banking information. Major Mobile Networks Operators (MNOs) in Kenya such as Safaricom, Telkom Kenya and Airtel Kenya, offer mobile money services namely: M-Pesa, Orange Money and Airtel Money respectively. Currently, 17 million users transfer Kshs. 2 billion daily, of which more than 14 million are M-Pesa customers. Mobile money service providers have partnered with commercial banks such as Equity Bank, I&M Bank, Kenya Commercial Bank, Barclays Bank, Commerce Bank of Africa and Co-operative Bank among others to provide high-quality financial products aimed at customers without bank accounts. The commercial banks target the unbanked customers via various channels. These channels include the Sim Tool Kit menu, Uninstalled Service Data (USSD), native Mobile Banking apps running on Android and iOS.

It is vital to note that access via these channels can be done anytime during the day and throughout the year. Customers of Financial Institutions need to access their funds in electronic wallets and physical bank accounts. Mobile Banking increases the access. Despite the potential of the mobile banking in enhancing financial inclusion, reducing the cost of banking and increasing convenience as asserted by (DR. Willy & Opili, 2015), increased access to financial information comes with challenges. Did you know that while enjoying financial services at the touch of your fingertips could come at a great price? Research has shown that mobile banking security threats are on the rise.

According to report by (Connect, 2018), 71% of mobile banking users have been victims of financial fraud. Out which 53% are mobile banking fraud. The reports further affirm that 83% of victims are willing to leave their current bank if their respective banks don’t do enough to protect them. These statistics clearly show that increasing bank frauds decrease customer confidence in banking products as a result of eroded perception and loses incurred. Therefore, mobile banking frauds damage the banks' relationship with customers and, as a result, loss of revenues.

Some of the challenges include but not limited to identity theft and account misuse as part of fraud. In addition, customers have suffered other losses from social engineering (Uppal, 2014).

A study conducted by (Luvanda, 2014) shows that mobile applications are prone to man in the middle attack. Further, a report done by (Associates, 2014) documents that phishing, spoofing and social engineering are some of the leading mobile banking threats.

According to (Alhuseen O. Alsayed, 2017) phishing refers to a criminal attack to steal sensitive information and it involves modus operandi to deceive consumers into thinking that their financial institution is asking for information from them, in which case, the request is from hackers. Theft of sensitive information leads to cyber identity theft, as it includes unauthorized personal or group having access to confidential information. Armed with confidential information, the impostor then approaches a mobile customer service provider with proof of originality, claiming that he had lost his handset or SIM damage with the intention of having a dual SIM card. A dual SIM card is used to register mobile banking or access a customer bank account as a result of customer losses.

In a report published by (Associates, 2014), social engineering is defined as a set of methods used to manipulate people into revealing confidential information. Although similar to a ploy of self-confidence or simple deception, the term commonly applies to the trickery of collecting information or accessing a computer program and in many cases the attacker has no direct contact with the victim. On the other hand, spoofing is an attack that involves a masquerader that changes the address field in the subject of an SMS message with a different alphanumeric thread. The message may appear to be genuine, yet from a genuine perspective, the outsider has altered it.

These challenges are real and can be eliminated by improving the authentication mechanism used by financial institutions. This can be achieved through use of multiple layers of authentication as asserted by (Sarhan, 2015).

Currently, mobile banking authentication is purely done through use of PIN. For instance: Mobile banking applications, such as: Eazzy banking App for Equity bank, KCB Bank App by Kenya Commercial Bank, and MCOOP Cash by Co-operative Bank Limited. Internet Banking for both retail and Cooperate use One Time Pin (OTP). Users key in PIN to log into mobile applications to complete transactions. According to (Connect, 2018), this makes an avenue for fraudsters to conveniently carry out transactions on behalf of the customers once a SIM swap has been done or social engineering has taken place. This has created a gap to be filled by employing an additional layer of authentication and authorization on mobile banking applications hence USSD push.

Therefore, this study intended to investigate how to overcome the weaknesses of using Personal Identification Number (PIN) as the only means to authenticate users on mobile banking channels and demonstrate the implementation of an additional layer of authentication and finally authorization for all transactions.

(Santovec, 2016) attests that PINs are easier to crack and mobile banking customers are at risk of receiving fake SMS messages and scams. In addition, the loss of a person's mobile device often means that criminals can access your mobile bank PIN and other sensitive information. Other challenges associated with PIN Shoulder browsing is a way of looking at someone's shoulder to get information. In a crowded environment, it is very easy and useful to stand next to a person and see how the PIN numbers are entered even on the card terminal or mobile device. Another challenge is fraud, which is impersonation, gaining access and using someone else's account. Another challenge is replay attacks. This kind of attack involves attackers spy on the conversation between the sender and the recipient and take important information e.g. share the key and then communicate with the recipient with that key. In a replay attack the attacker gives proof of his identity and credibility.

The aforementioned risks and challenges associated with PIN formed the fundamental problem to be solved by this research. The question that this research strived to address was: How does USSD push enhance mobile banking security when implemented together with other factors of system authentication.

The additional layer of authentication is hereafter referred to as Multi Factor Authentication (MFA). This involves use of a customer’s PIN for logging in and another authentication mechanism to allow completion of financial transactions irrespective of the channel. USSD gives a session-based service that offers simple interaction through a menu driven data interface on a user device. It works on all GSM handsets with messages sent directly over the network signaling channels, which means it does not require application installation. It is more secure than use of OTP which is SMS based.

1.2 PROBLEM STATEMENT

In the recent past, reduced cost mobile phones led to increased number of mobile subscriber base in Kenya. Financial service providers such as banks and financial technology companies have taken advantage of this growth avail mobile financial services such as bill payments; funds transfer etc. to their customers. The financial institutions have enforced a requirement for their customers to register to the mobile banking service before they can enjoy the digital product offerings. This registration process typically involves the use of a parameter owned by the customer and known by the financial services provider which is the mobile number.

Upon successful registration, users get a four digits' personal identification number (PIN) with which they can transact with. A typical mobile based financial transaction involves the customer logging in to the mobile device using their secret PIN. Once authentication is completed successfully, the customer can then initiate and complete a financial transaction such as bill payment. Please note that in this case, the authorization of individual transactions happens as long as the user was authenticated successfully using the PIN. Therefore, any entity or individual who has acquired a customer's PIN can initiate and successfully complete a transaction once they have been logged into mobile banking application. Hence there is a need to challenge the transactions initiated on mobile banking channels. The question that this research strived to address was: How does USSD push enhance mobile banking security when implemented together with other factors of system authentication?

1.3 RESEARCH OBJECTIVE

The objective of the study was to investigate the challenge of using PIN as the only factor of authentication when doing transactions on mobile banking applications and provide a solution to ensure secure mobile banking transactions by offering out of band USSD push. This solution would offer increased security as it would not only be user dependent but also tied to other details such as International Mobile Equipment Identity (IMEI), Mobile Systems International Subscriber Identity Number (MSISDN), and International Mobile Subscriber Identity (IMSI) in addition to time bound USSD push in addition to biometric authentication where applicable. The solution implemented offers remedy to the challenges aforementioned leading to mitigation of financial losses incurred by customers of Banks in Kenya.

1.4 SPECIFIC RESEARCH OBJECTIVES

I. To determine the need of an additional layer of security in mobile banking transaction

II. To develop model that is cost effective, efficient and secure for mobile banking transactions.

III. To develop a mobile banking application prototype that demonstrate end to end secure mobile transactions.

IV. To evaluate the effectiveness of incorporating a combined USSD push and PIN for a time efficient multifactor authentication.

1.5 RESEARCH QUESTIONS

I. What were the security challenges in mobile banking transactions as a result of using PIN as the only factor of authentication and authorization?

II. What were the alternative to current mobile banking security models when doing transactions?

III. How to use USSD push to enhance mobile banking security when implemented together with other factors of systems authentication?

IV. How the proposed system could be designed and implemented to address the highlighted mobile banking security issues?

1.6 JUSTIFICATION

The findings in this research report are significant to various stakeholders in the Kenyan Banking sector.

I. Help reduce losses incurred by Commercial Bank customers' by implementing an additional layer of transaction authorization.

II. Increased revenue stream for financial institutions as more customer's uptake mobile baking channels since they are likely to have increased confidence in financial systems.

III. The knowledge gained is vital in reevaluating and redesigning the mobile banking systems to achieve a reduction on the risks and enhance uptake of mobile banking leading to growth of the financial institutions.

1.7 SCOPE OF STUDY

The study focused on evaluating the mobile banking applications in relation to authentication and authorization by mobile banking customers in Kenya. The study was limited only to banks in Kenya.

1.8 LIMITATION OF THE STUDY

The limitation of the project was on getting information on the current mobile banking authentication methods and the real challenges faced by mobile banking customers. Most financial institutions were not willing to provide this information. Therefore, the research collected data directly from customers.

1.9 DEFINITION OF TERMS

The following terms have been identified in the report;

1.9.1 RISK

This is the possibility of loss or something unpleasant happening because of use or association with a given technology or item.

1.9.2 FINANCIAL INSTITUTIONS

These are corporate organizations that provide financial services such as accepting deposits, creating business loans and providing basic investment products.

1.9.3 MOBILE BANKING

This is the provision and execution of banking and financial services through the help of mobile telecommunication devices such as the telephone or tablets.

1.9.4 USSD

Unstructured Supplementary Service Data is a global system for communication technology used to send text between a digital phone and an application program on the network.

1.9.5 IMEI

This is a 15-digit distinctive number used to identify each phone on a GSM network. IMEI is usually incorporated in the cellular phone.

1.9.6 IMSI

International mobile subscriber identity refers to a number that uniquely identifies a user of a cellular network.

CHAPTER 2 : LITERATURE REVIEW

2.1 INTRODUCTION

Mobile phone verification is a mandatory requirement for all mobile banking services providers. Mobile Bank Verification correctly identifies the user to access mobile banking systems as described in (Connect, 2018). Most mobile applications verify the use of PIN and MSISDN while native apps can have additional proof of installation made on the feature of things like Front Camera and finger readers (Antal & Szabó, 2015). The security level of a given authentication system depends on the combination of responsibility, authentication channel, authentication storage, and encryption.

A good number of studies have been conducted on cell-based validation and their level of security. These researches were on areas such as PIN authentication, Multifactor authentication: Two Factor Authentication or three factors authentication. All these authentication mechanisms rely on telecommunication infrastructures provided by Mobile Network Operators (MNO). This inquiry project proposed a blend of various factors such as PIN, USSD push and other unique features of a device of SIM card for secure authentication and authorization.

2.2 MOBILE BANKING AUTHENTICATION MECHANISMS

2.2.1 Mobile Banking Personal Identification Number

Mobile-Banking PIN is made up of four numbers and is stored on the SIM card currently inserted in the mobile device. Every time a mobile banking customer logs into mobile banking application, the PIN is checked against stored values on the application databases. Next section describes the most common implementation of M-Banking PIN authentication mechanism.

2.2.2 Single-Factor Authentication

Single-Factor-Authentication (SFA) refers to a mechanism of using only one attribute of authentication to allow or reject access to a banking service according to (Schneier, 2019). In context of PIN, this is however not possible to be enforced from system perspective and rarely do customers remember to change their PINs regularly.

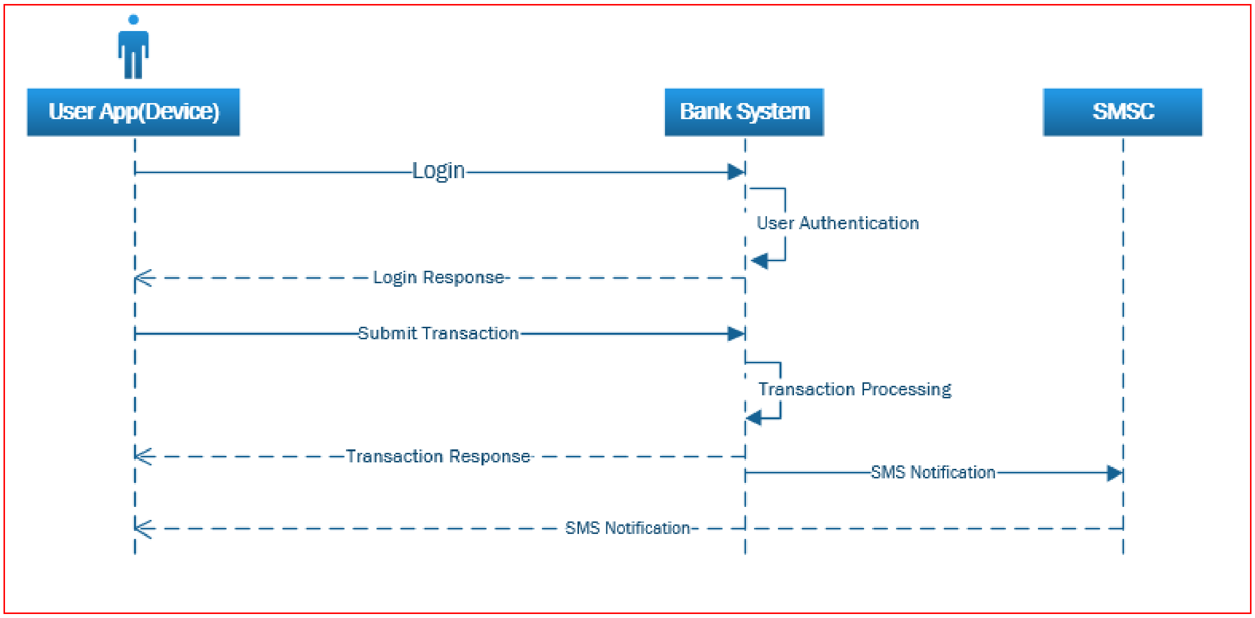


Figure 1. High-level single factor authentication (adapted from Finserve m-banking flow 2019)

Table below 1 describes a high-level system flow for a single factor authentication mobile financial system.

STEP	DESCRIPTION
Login/Authentication Request	This represents the login/authentication request from a mobile financial system channel. An example is when a customer logs in to a banking web portal by providing the login credentials.
Authentication	This involves the mobile financial system authenticating the customer based on the credentials provided
Login/Authentication Response	This is the action displayed to a successfully authenticated user. An example could be a user is able to view the transaction page in a web portal or a user is successfully logged in to the banking mobile application
Customer transaction request	This is the customer-initiated transaction such as bill payment
Transaction processing	Mobile financial system processes the transaction. This could involve funds transfer, bill payments, airtime purchases etc.

Customer transaction response	Once the financial system completes the transaction, the customer gets notified of the successful/failed transaction. This could be in the form of an SMS, popup or even an email.

Table 1: Pin Authentication Steps

2.2.3 Two-Factor Authentication Using One Time PIN (OTP)

This implementation of authentication involves the use of customer PIN and another parameter generated by the financial service provider known as One Time PIN (OTP). The OTP is generated as part of the transaction flow and send to the customer as an SMS. The customer will then key in the received OTP in order to validate and authorize the transaction.

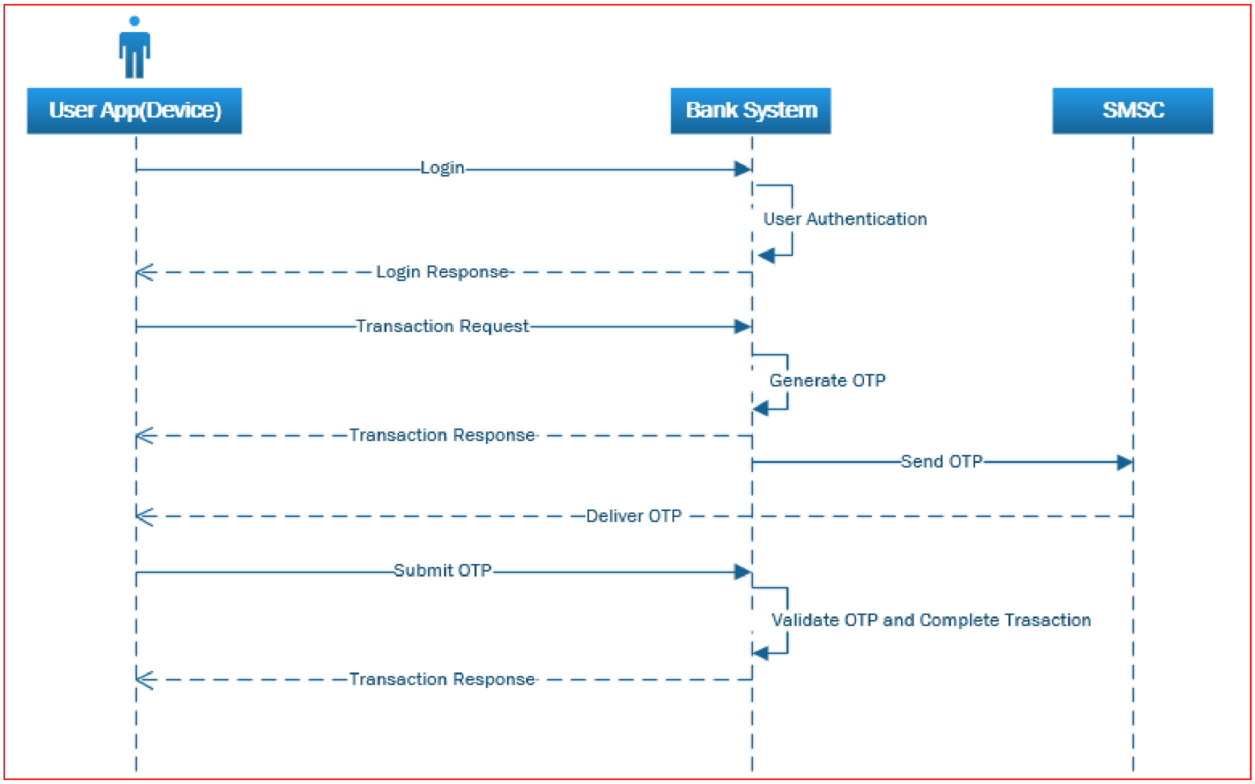


Figure 2. High-level 2-FA using PIN and OTP (adapted from Finserve m-banking flow 2019)

Below is a description of the Figure 2 flows;

STEP	DESCRIPTION
Login/Auth Request	A customer logs in to a mobile financial system using their PIN. A typical example is when a customer logs in to their internet banking portal.
Authentication	The mobile financial system authenticates the customer based on the credentials provided by customer during login.
Login/Authentication Response	This is the action displayed to a successfully authenticated user. Example is when the customer is able to view the transaction pages on their internet banking portal.
Customer transaction request	A customer-initiated transaction request such as bill payment, funds transfer, airtime purchase etc.
OTP generation	The mobile financial system receives the transaction request and then initiates the request. As opposed to the single factor authentication scheme, the financial system does not complete the transaction. Instead, it generates an OTP which uniquely identifies the transaction and sends to the customer. The transaction then goes to an intermediate state such as 'pending'.
Send OTP	The mobile financial system securely submits the OTP which is basically an SMS to the Short Message Service Centre (SMSC) of the telecom provider. Some of the parameters provided by the mobile financial services provider are the recipient's mobile number and the source address. The source address is whitelisted specifically for the financial service provider by the telecom provider.
Deliver OTP	The telecom provider will then deliver the SMS to the subscriber who happens to be accessing financial services. The subscriber will be able to confirm the originator of the OTP based on the source address in the SMS.
Submit OTP	This section involves the customer submitting the OTP to the mobile financial system. The customer could be manually typing on the internet portal or manually entering on a mobile application.

OTP validation	Once the mobile financial system receives the OTP, it performs a number of checks such as: • Validity of the OTP • Time validity (an OTP has time duration tied to it) If the above checks are passed, the transaction that was in pending state is then completed. This is the authorization phase in the flow.
Transaction Response	The financial system notifies the customer using the desired channel such as SMS, Email, Popup etc.

Table 2: 2FA using PIN and OTP

The above scheme of using OTP for two-factor authentication has been implemented by financial services in Kenya however it has a couple of challenges. First, the OTP delivery is dependent on the telecom provider's network. If the network coverage is poor, there is a high possibility of the OTP delivery failing. Secondly, the SMSC works on a store-and-forward mechanism which is tied to a retry schema. If the delivery fails on the first attempt, the retry could happen way after the expiry of the OTP. Lastly, if someone has access to the SMSC, it is possible for the OTP to be intercepted in a typical man in the middle attack (Alhuseen O. Alsayed, 2017).

The USSD implementation of multifactor authentication tried to address the above shortcomings of the OTP as can be illustrated in the next section under the proposed model.

2.2.4 Biometric Authentication

Biometric technology uses different physical or behavioral unique patterns of users to determine authenticity or identification. Smartphones and other devices are becoming more widely distributed with biometric scanners already fitted. In addition to, the aforementioned scanner, there is a growing number of services that call for higher security and better customer experience therefore traditional authentication methods (e.g. passwords and PINs) are progressively being replaced by biometric technology. according to (Anil K. Jain, 2008). Any biometric system requires three main components: A sensor that captures the feature, a biometric application to compute and compare features, and a database to store a template as document by (Julian Fietkau, 2020). Biometric Authentication sensors continue to develop and the authentication mechanisms (algorithms) to help in device unlocking also mature. These advancements have helped in reducing False Rate Acceptance (FARs) and block attempts on spoofing as documented at (Samsung, 2020).

Face, Iris, pattern, and voice recognition are great authentication mechanism that can be implemented in mobile banking authentication. However, there limitations with each of them. Executions of face recognition that don't map the face in three dimensions can possibly be spoofed utilizing a photograph of the client, while even refined facial recognition advances have a higher FAR than a considerable lot of the progressed biometric confirmation alternatives talked about beneath. Likewise, facial recognition is inclined to bogus negatives. This alludes to when your gadget neglects to open due to wearing glasses or cosmetics, or only because of contrasts in encompassing lighting. Security-cognizant associations dealing with touchy information ought to consider unique mark or iris examining for more noteworthy insurance. This is as indicated by (Samsung, 2020). Iris examining utilizing an infrared sensor offers an incredibly elevated level of security and permits clients to "open with a look," in any event, when in a hurry or wearing gloves. Your iris is an amazingly information rich physical structure and contains an example that is extraordinary to every person and for all intents and purposes difficult to reproduce. Furthermore, since eyes are self-cleaning and picture capture is performed without physical contact with the user, readings are exceptionally exact and dependable. Contrasted with facial recognition, authenticating on a device using iris filtering is generally slightly slow, as the client must adjust eyes to the infrared sensor while holding the gadget 10 to 14 inches from the face. Moreover, iris checking can be influenced by wearing glasses or contact focal point. Splendid daylight can likewise prompt bogus negatives because of infrared clamor as archived at (Samsung, 2020). Unique finger impression verification is the way toward coordinating fingers dependent on the structure of the upper skin. In as much as possible offer fingerprints with another, research has indicated that fingerprints are likewise helpless against assaults. As per (Julian Fietkau, 2020)fingerprints can be separated from photographs or duplicated from contacted objects like espresso cups, consoles, and different things. There are two significant worries over biometric frameworks when contrasted and secret-phrase based verification frameworks. To begin with, biometric attributes can't be repudiated and reissued in the situations where they are undermined. For instance, if an individual's unique finger impression picture is taken, it is absurd to expect to supplant it like supplanting a taken secret key. In addition, various applications may utilize the equivalent biometric characteristic; if a foe secures a person's biometric attribute in a given application, the adversary may utilize the fingerprint to gain access to different applications. Secondly, finger prints are not entirely clandestine. A targeted customer may have left their unique mark on any surface they contact which can then be harvested and used elsewhere on behalf of the customer. This is as indicated by (Stephen J. Tipton, 2014). To this end, biometric confirmation alone isn't viable as a factor of verification for portable financial exchanges. Utilizing PINs and Passwords as the sole security choice position customers as obvious objectives for misrepresentation. Numerous associations are currently considering multifaceted validation (MFA) by consolidating a unique mark with either retina, voice, or facial recognition or PIN, for instance. MFA makes it incredibly hard for a hacker to penetrate client accounts. This security strategy consolidates something a client is and something a client knows. Portable financial clients will probably observe biometric recognition combined with PINs and passwords for two-considered verification as per (Dossey, 2019).

2.3 CONCLUSION

The literature reviewed agreed with the need to verify the authenticity of multiple items using more than two attributes (an attribute known by the user, attribute that the user has, and attribute that the user is) in mobile banking solutions. And in the review of the literature, all researchers point out that the authenticity of a single object using a PIN is weak and dangerous. Research work has been done on the validation of customers or users via multi-factor authentication by use of more than one attribute. The research work, however, fails to have a combination of attributes that use a combination of standard authentication methods, unique mobile attributes, and USSD push to increase the security of banking solutions. Most investigators used biometric fingerprints and iris and PIN / Passwords. However, the researchers did not address the risks associated with a PIN such as unauthorized SIM swaps. Device specific details associated with the USSD push was proposed as a solution to the research gap identified in the reviewed literature. In addition, there is need to combine multiple factors of authentication to help in enhancing mobile banking security. In this study we demonstrated use of USSD push, PIN and Fingerprint to enhance mobile banking security. This kind of multifactor authentication makes it impossible to compromise mobile banking user while they enjoy seamless mobile banking transactions.

2.4 CONCEPTUAL FRAMEWORK

The procedure of thinking and choosing a research topic, the selection and use of research strategy and methods of data collection and generation, data analysis and draw conclusions, including identifying any limitations in research is referred to as conceptual framework. (Oates, 2006).

The illustration below shows the relationship between dependent and independent variables used in the research. A number of functionalities were built into the application including USSD push interface, PIN, device specific token to realize a secure mobile banking model. These variables were used in the mobile payments system by users directly or indirectly when doing log in and authorizing transactions. The security of the mobile banking solution was based on the authentication factors complexity, channels used for communication and the cryptographic patterns used.

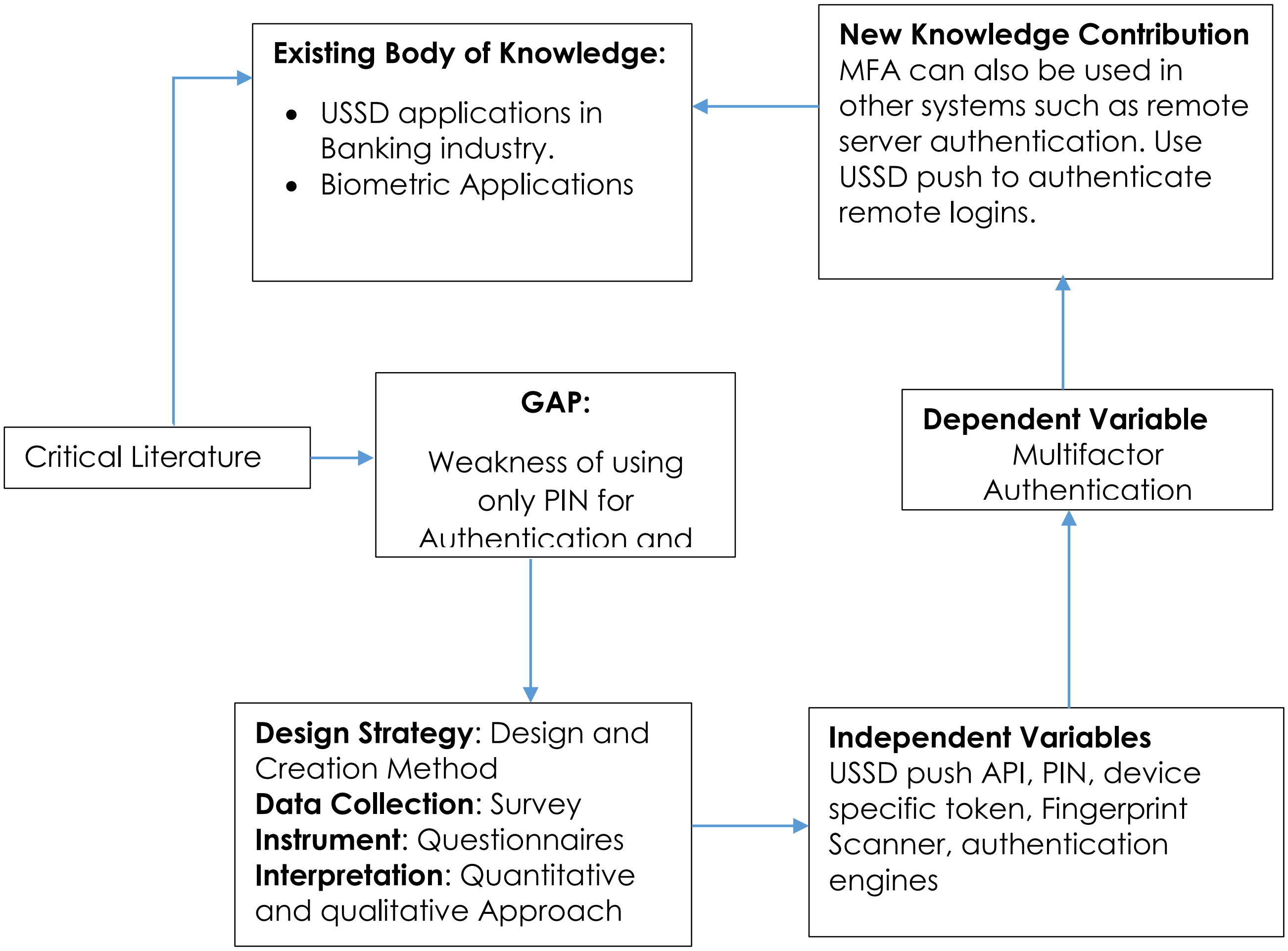

Existing Body of Knowledge:
USSD applications in Banking industry.
Biometric Applications
New Knowledge Contribution
MFA can also be used in other systems such as remote server authentication. Use USSD push to authenticate remote logins.
Critical Literature
GAP:
Weakness of using only PIN for Authentication and
Dependent Variable
Multifactor Authentication
Design Strategy: Design and Creation Method
Data Collection: Survey
Instrument: Questionnaires
Interpretation: Quantitative and qualitative Approach
Independent Variables
USSD push API, PIN, device specific token, Fingerprint Scanner, authentication engines

Figure 1 Conceptual Framework

2.5 THE PROPOSED MODEL

2.5.1 Multi-Factor Authentication (MFA)

In this authentication mechanism, three attributes are employed to successfully verify a given user: an information factor ("something known only the user"), a ownership factor ("something only possessed by the user"), or integral factor ("a factor that defines only the user") as written by (Adeoy, 2012). This model employs three parameters to implement multi-factor authentication. The customer's PIN and/or fingerprint for authentication, a token, IMSI and a USSD push for transaction authorization.

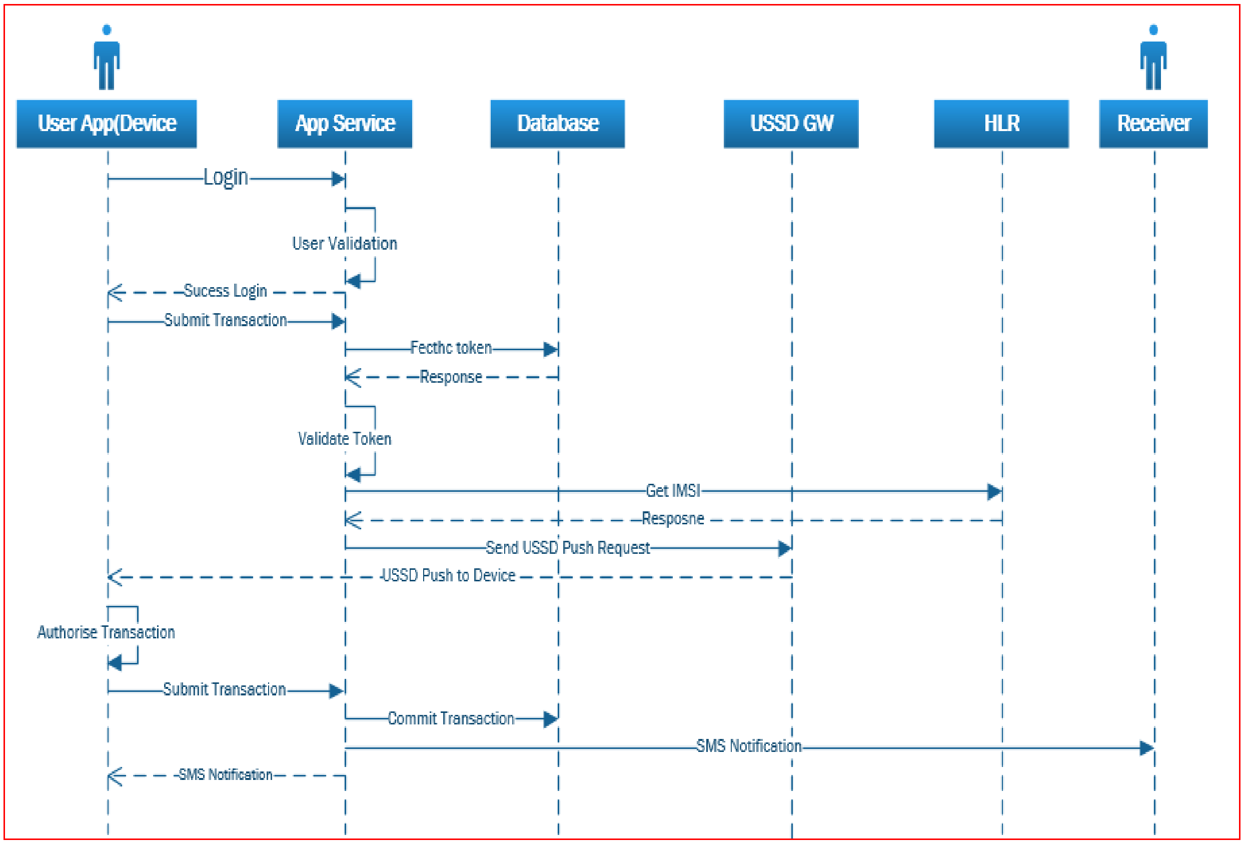


Figure 2 High-level MFA using PIN, token and USSD Push

Table 3 Describes the steps involved in MFA, token and USSD push

STEP	**DESCRIPTION**
Login/Auth request	A customer logs in to a mobile financial system using their PIN. A typical example is when a customer logs in to their internet banking portal. Fingerprint authentication also happen on the user device if the device supports Fingerprint reading and authentication.
Authentication	The mobile financial system authenticates the customer based on the credentials provided by customer during login.
Login/Authentication Response	This is the action displayed to a successfully authenticated user. Example is when the customer is able to view the transaction pages on their internet banking portal.
Customer transaction request	A customer-initiated transaction request such as bill payment, funds transfer, airtime purchase etc.
Validate and Generate USSD push	The mobile financial system securely submits the request to the telecom USSD gateway. The key parameters in the USSD Push are the session identifier, recipient mobile number, token and the USSD content. The session identifier is time based and hence expires within a set period. Token is a combination of IMEI and Device ID.
Deliver USSD Push	The mobile financial system receives the transaction request, initiates transaction and generates a USSD push to be submitted to the customer. The contents of the USSD menu are a question that requires the customer to respond to. Example: ***"Do you want to complete transaction of KES 5000 to Account 445566 Account Name: Mary Jane?*** ***1. Yes*** 2. ***No***" The mobile system then opens a connection, initiates a session and submits the request to the telecom USSD gateway to be submitted to the Bank System.
Submit USSD Response	The customer selection is forwarded from the customer device to the Telecom USSD gateway within the same session.
Deliver USSD response	The telecom delivers the customer response to the financial service provider using the same connection that had been opened for the USSD session
Validate and complete transaction	Once the financial service provider has received the customer selection, they can then do either of the following. 1. Complete transaction if the info provided is sufficient 2. Cancel transaction if the user has chosen **No**.

	With this, we achieve authorization on a different channel(out of band) from the one used to initiate the transaction.
Transaction Response	The financial system notifies the customer using the desired channel such as SMS, Email, Popup etc.

Table 3: MFA Using USSD Push

The implementation of USSD to achieve multi-factor authentication provides the following gains;

- The authentication and authorization can happen in different channels. Out of band.
- The USSD is session based hence the chances of replay are mitigated or greatly reduced.
- The USSD push can only be received by the mobile number that is registered on mobile banking platform hence minimal chances of identity theft as the MSISDN is also verified in Home Location Register (HLR) in GSM.
- USSD can be implemented across all devices
- USSD does not need data to operate hence can be accessed anytime.

USSD push to pre-registered MSISDN and handset can be done as part of an account authentication, a verification for, a transaction confirmation, or as part of validation in high-risk transactions. This is according to (Corella & Lewison, 2012).

2.6 Conceptual Architecture

The conceptual architecture depicted systems components, communication between the various components, data encryption, authentication and authorization. Data Security adhered to Open Web Application Security Project (OWASP) and ISO/IEC 27000:2018 for information security management systems (ISMS).

2.6.1 ISO/IEC 27000:2018

Based on((27000:2018, 2018) the following standards were conformed to in the architectural design and consequent implementation of the prototype development.

Issues addressed include;

2.6.1.1 Authentication Scheme

The design allowed ascertaining that a given principal is who they claim to be whenever they want to access a given asset. For instance, users and application are authenticated against credential by the database server. The scheme employed use of IMEI and device ID to generate a token that was used to authenticate with HLR in generation of USSD push for every transaction.

2.6.1.2 Confidentiality

The conceptual architecture ensured confidentiality by granting access to database to only authenticated principals (27000:2018, 2018). To ensure confidentiality, encryption mechanism known as **Bcrypt** was used to hash sensitive information for both data at rest and on transit thereby adhering to OWASP guidelines for web applications. The architecture employed Bcrypt algorithm that is implemented in two stages. In the first stage, Eksblowfish's setup is called to initialize eksblowfish's state with the cost, the salt, and the password. Considerable Bcrypt's time is spent in the luxurious key schedule. The next stage involves 192-bit value being encrypted 64 times. This require using eksblowfish in ECB mode with the state from stage one. The outcome is usually the cost and 128-bit salt concatenated with the result of the encryption loop as documented at (usenix.org, 2020).

2.6.1.3 Availability

The conceptual architecture employed the Representational State architecture. This ensured that the system developed is scalable horizontally in cloud environment such as Azure Cloud or any other cloud solution. The overall goal was to have an accessible system on demand at all times.

2.6.1.4 Integrity

Refers to maintaining data in its original form without unauthorized modification. This has been ensured by use of referential integrity checks placed at the database level. Only authorized alteration can be performed and the alterations are cascaded to all entities in all relations within the database.

2.6.1.5 Authorization Standards

Finally, In the conceptual architecture, only authenticated users and applications were allowed to access various assets in the system. Meaning the architecture design ensured that access to assets is authorized and restricted based on operational and security requirements.

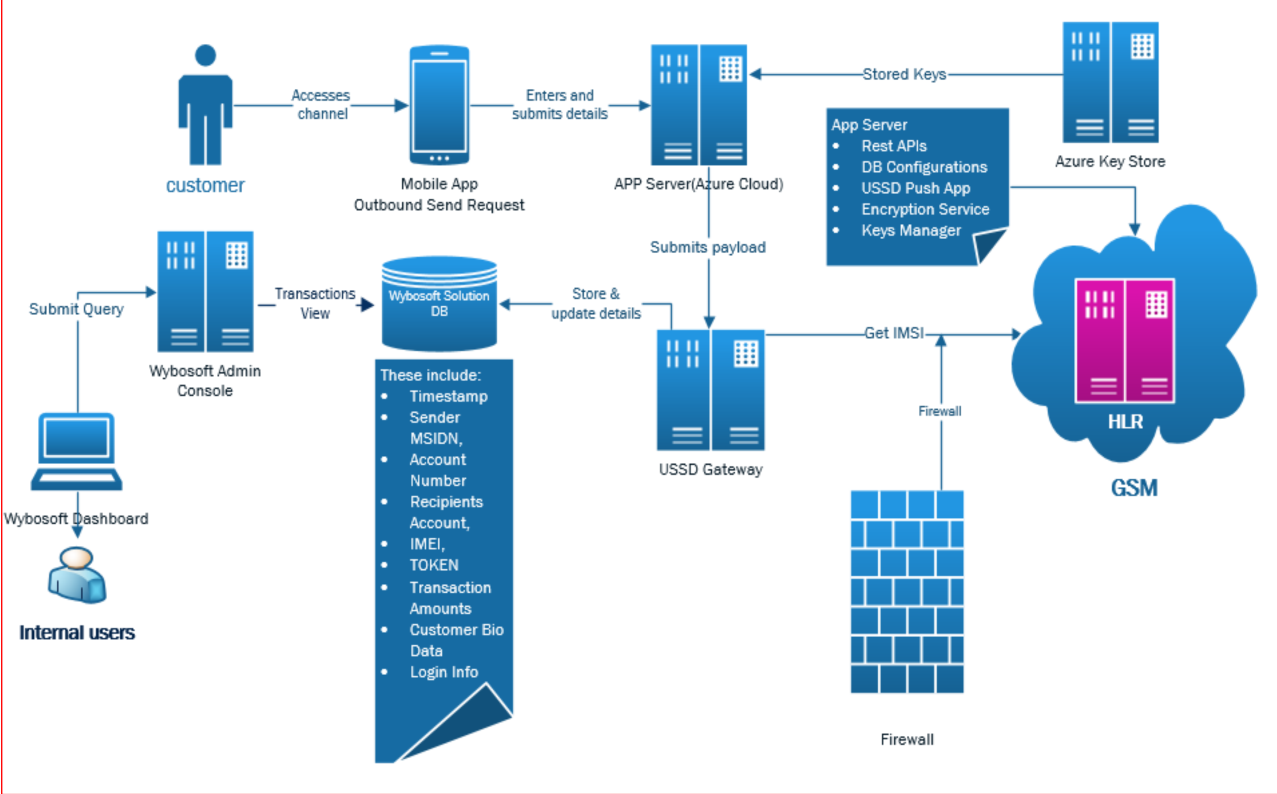


Figure 3: High Level Conceptual Design, Wybosoft Bank

CHAPTER 3 : RESEARCH METHODOLOGY

3.1 INTRODUCTION

This section defines the exploration design, data collection procedure, participants, research procedure, research instruments used and their validity of the together with their reliability. The section further describes data analysis and the statistical methods that were used to analyze the collected data as well as interpretation of data.

3.2 RESEARCH DESIGN

The research design included strategy, analysis of records, simulation, method of data collection and research process was highly structured. It defined size of sample and the nature of sample analysis whether qualitative or quantitative (Cooper & Schindler, 2014). This section clearly defined how various methods and techniques were used to realize the fulfillment of objectives highlighted. The research design led to establishment of basis for developing a system to demonstrate the use of USSD push.

3.2.1 Population

A population represents a set of items, people or animals who share common characteristics that are to be studied according to (Israel, 2018). The study population consisted of mobile banking users in Kenya.

3.2.2 Sampling Technique

The study's target population was comprised of mobile banking users in Kenya. This study employed non-probabilistic sampling methods. The researcher used convenience non-probability method to identify a subset of the population. The convenience method was used because of ease to reach the respondents within Kenya and the tool of data collection chosen was also greatly supported by convenience sampling. In addition, Snowball Sampling was used since we relied on some of the initial respondents for referrals to the next respondents. Also the costs associated with this method are significantly lower, and we ended up with a sample that was very relevant to the study.

3.2.3 Sample Size

A sample size is a proportion of the entire population in statistics. Cochran formula was used in the research to compute an ultimate sample size based on a desired level of accuracy, anticipated level of confidence and the projected percentage of the attribute present in the population as describe in (Israel, 2018).

$$n_0 = \frac{Z^2pq}{e^2}$$

Figure 4: Cochran Formula for determining Sample Size

Where:

- **e** is the level of accuracy needed (i.e. the margin of error acceptable),
- **p** is the approximation of populace proportion which has the attributes in question
- **q** is **1 – p**.
- **Z** values can be obtained from Z-table.

For instance, mobile banking users in Kenya are 17 million according to (CBK, 2016). In the research a representation or sample size was calculated as p = 0.5 at confidence level of 95% with at least 5 percent—plus or minus accuracy. A 95 % confidence level translate to 1.96 Z values as per the normal tables, Therefore, we have:

((1.96) ^2 * (0.5) ^2) / (0.05) ^2 = 385 respondents from the target population. A total number of record 442 responses were received. See annex of the link to responses link

3.2.4 Research Procedure and data collection method

A preliminary study was conducted to test the effectiveness of the data tool in collecting the right information sought from the respondents. Particularly the pilot sought to identify whether the respondents understood the questions as intended. The pilot study helped in identifying ambiguous questions and words for review before the actual study. The study used twenty respondents of the sample size to participate in the pilot study. The participants used for the pilot study were excluded from the final study to eliminate preconceived opinions about the study. The data collection process adopted online survey administered via google forms.

3.2.5 Data collection tool

The research used a questionnaire as an instrument to collect information so as to establish the cases and instances of mobile banking risks. It was also used to explore the need for USSD push as mobile banking authentication mechanism. The questionnaire had two sets of questions. Five point Likert questions and open ended questions. Use of Likert type of questions ensured focus in answering of the questions. On the other hand, open ended questions created more depth and clarification on the respondents' opinions.

The respondents were reached by sending a google forms questionnaire link to emails and snowballing sampling helped in creating awareness of the survey to reach other respondents as well. The respondents were given a window of 10 days to complete the questionnaires. Since the survey was online, real-time data was analyzed quickly and efficiently.

3.2.6 Reliability of the Data Collection Tool

The instrument of survey must ensure that the data it captures can be relied upon by the researcher. Therefore, reliability in the context of the research was the degree to which the tool measured the data collected (Biddix, 2019). Consequently, instrument of data collection employed was questionnaire. It was pre-tested after design then eventually used. In this study, a high level of reliability was achieved using various approaches: The response rate was increased through personal distribution of the questionnaires and collected on completion after a short while.

3.3 RESEARCH SCHEDULE

The duration of the research was six months. This was undertaken as a project. The research schedule has been attached on appendix A.

3.4 ETHICAL CONSIDERATION DURING THE RESEARCH

Prior to the implementation of the research design and methods discussed in this study, pre-data comparisons were made to ensure that no issue could arise to ensure the validity of the study. The study ensured that user information was kept confidential and no personal data about their conduct of banking activities and behavior was made accessible to other users or other respondents. This was achieved by conducting a research study or informal discussion with participants about their needs, informing them of the general purpose of the study and obtaining appropriate approval.

CHAPTER 4 DATA ANALYSIS AND INTERPRETATION

4.1 Introduction

Computation of specific descriptive statistics and measures along with searching for patterns of relationship that exist among the data groups was carried out. Since the data collected was quantitative, the best method to analyze this data was the quantitative method.

The data was first coded and entered in Statistical Package for Social Sciences (SPSS) for quantitative analysis. The application was also used to tabulate the data for presentation. Descriptive data analysis methods were then used to establish meaning from the data. Measures of central tendency, frequencies and variances were used to summarize the findings into concrete information for drawing conclusions. The data is presented by use of graphs and tables for ease of understanding. The understanding formed a basis for developing a system prototype to demonstrate the use of USSD push to enhance mobile banking security leveraging GSM technology.

4.2 Data Analysis

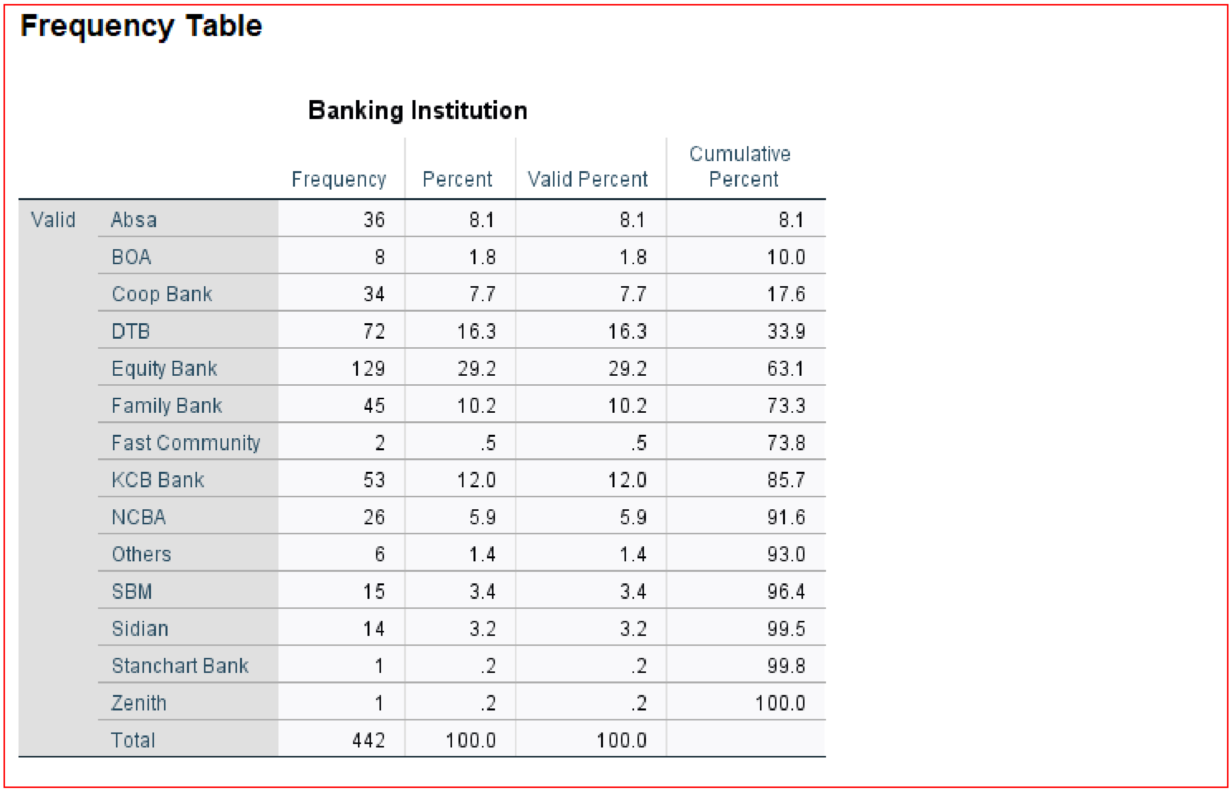
A mobile banking customer will always be in need of funds to carry out personal goals in life. As such a survey was done to ascertain the frequency of usage, challenges and the possible improvements they would want to see made to the mobile banking applications.

4.2.1 Survey

The survey noted that a number of mobile banking challenges such as social engineering is real and most customers have suffered losses as a result of compromised pins. The other challenge was mobile banking Sim card replacement. The challenge with one time pin also established to be a mobile banking issue. The survey went ahead and unearthed the other issues such as need for additional layer of authentication. The survey was completed by 442 respondents as stated earlier from various tier one and tier two banks Kenya. The sample questionnaire used is attached on appendix C. The analysis was done in the following section under frequency distribution tables.

4.2.2 Frequency Distribution Tables.

A total of 14 banks were represented in the survey. There are a total of 40 commercial banks in Kenya. This is according to (CBK, 2016). Therefore, a margin of **5%** and confidence level of **95%** for the population size, the research concludes that banks in Kenya were well represented in the research. This is portrayed in the figure below.



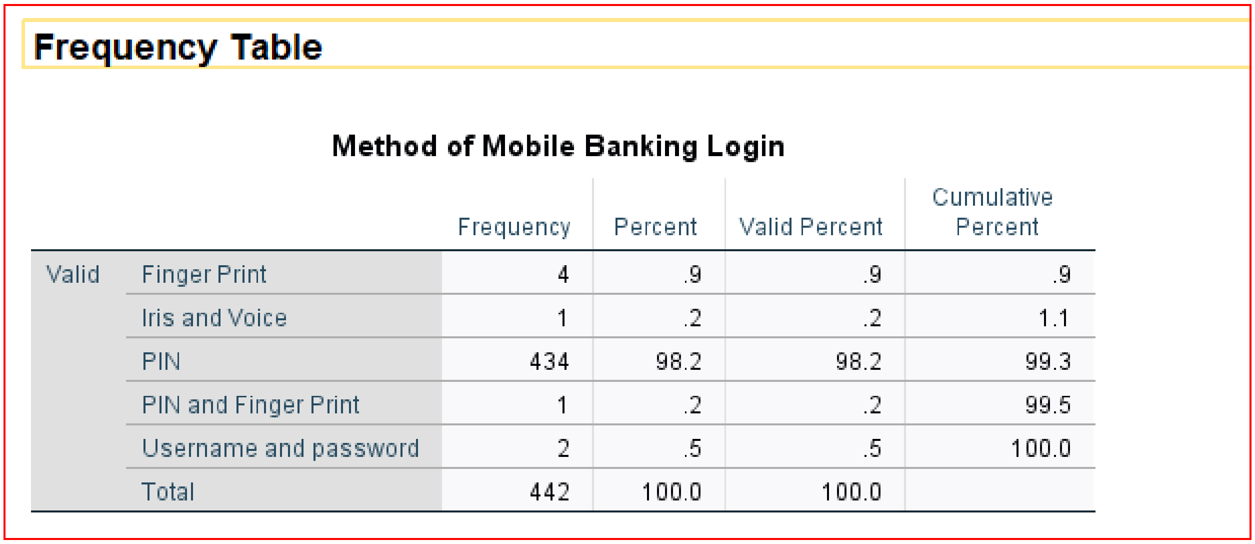
Frequency Table

Banking Institution

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Absa	36	8.1	8.1	8.1
	BOA	8	1.8	1.8	10.0
	Coop Bank	34	7.7	7.7	17.6
	DTB	72	16.3	16.3	33.9
	Equity Bank	129	29.2	29.2	63.1
	Family Bank	45	10.2	10.2	73.3
	Fast Community	2	.5	.5	73.8
	KCB Bank	53	12.0	12.0	85.7
	NCBA	26	5.9	5.9	91.6
	Others	6	1.4	1.4	93.0
	SBM	15	3.4	3.4	96.4
	Sidian	14	3.2	3.2	99.5
	Stanchart Bank	1	.2	.2	99.8
	Zenith	1	.2	.2	100.0
	Total	442	100.0	100.0	

Figure 5: Banking Institutions in Kenya

The figure below shows distribution and percentages of respondents' method of login into their respective mobile banking apps. **98%** login using PIN alone. Only insignificant number use other means such as username and password, fingerprint and PIN combined or Iris and Voice.



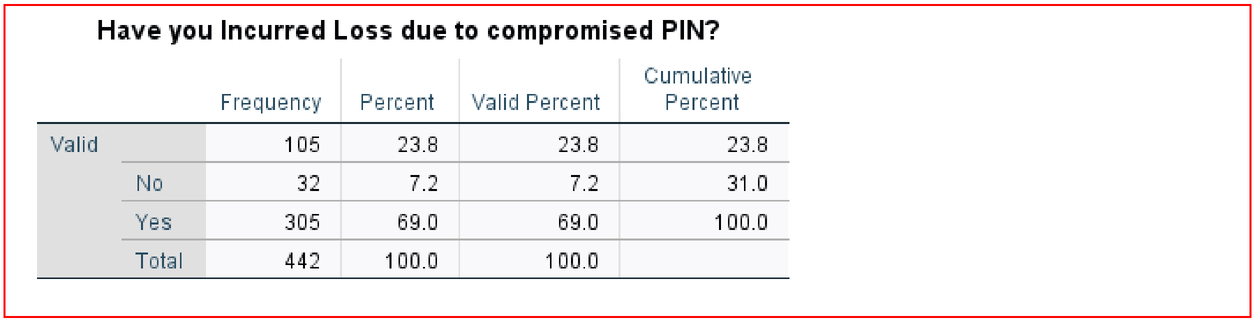
Frequency Table

Method of Mobile Banking Login

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Finger Print	4	.9	.9	.9
	Iris and Voice	1	.2	.2	1.1
	PIN	434	98.2	98.2	99.3
	PIN and Finger Print	1	.2	.2	99.5
	Username and password	2	.5	.5	100.0
	Total	442	100.0	100.0	

Figure 6 Mobile Banking Login Methods in Banks

The figure below shows distribution and percentages of respondents who have incurred losses as a result of compromised PINs. **69%** have incurred losses while only **7.2%** have not experienced any loss**. 23.8%** did not respond.

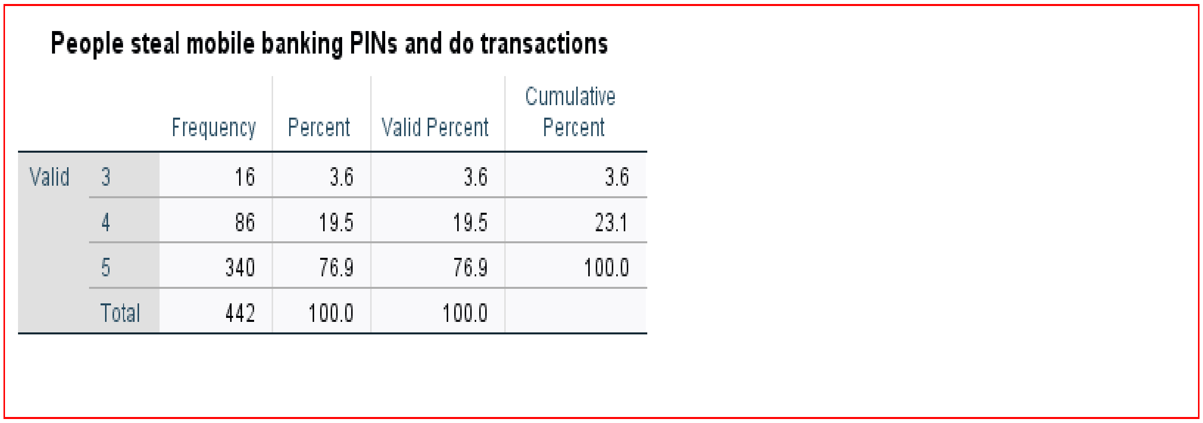


Have you Incurred Loss due to compromised PIN?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		105	23.8	23.8	23.8
	No	32	7.2	7.2	31.0
	Yes	305	69.0	69.0	100.0
	Total	442	100.0	100.0	

Figure 7: Losses incurred as a result of Compromised PINS

The figure below shows distribution and percentages of respondents on the level of their belief that people steal mobile banking PINs and then do transaction on behalf of customers. **76.9%** strongly agreed, **19.5%** agreed while **3.6%** were neutral.

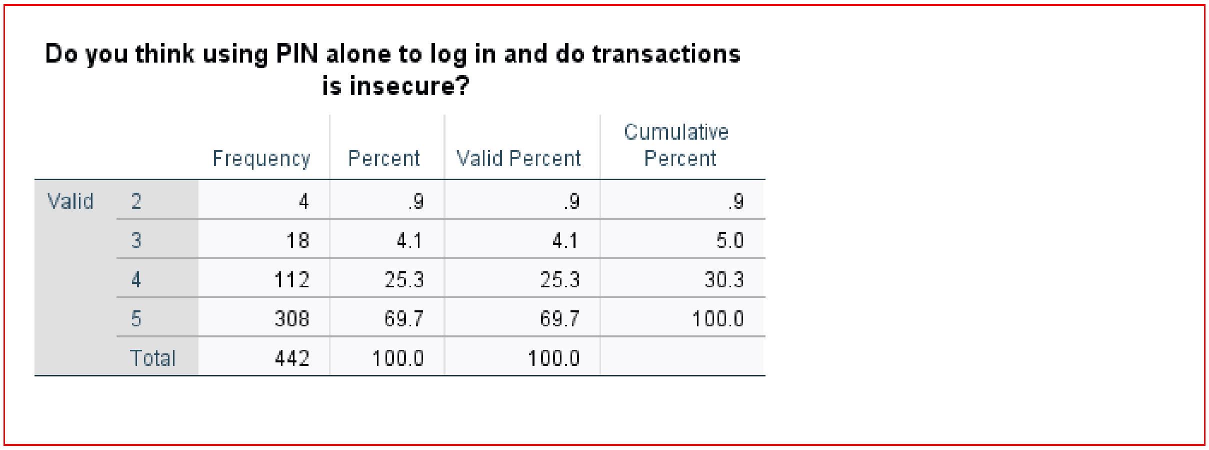


People steal mobile banking PINs and do transactions

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	16	3.6	3.6	3.6
	4	86	19.5	19.5	23.1
	5	340	76.9	76.9	100.0
	Total	442	100.0	100.0	

Figure 8: System based losses as a result of compromised PIN

Figure 9 shows distribution and percentages of respondents on the level of their thoughts that using PIN alone to log in and do transaction is insecure. **66.7%** strongly agreed, **25.3%** agreed, **4.1%** were neutral while **0.9%** did not agree.

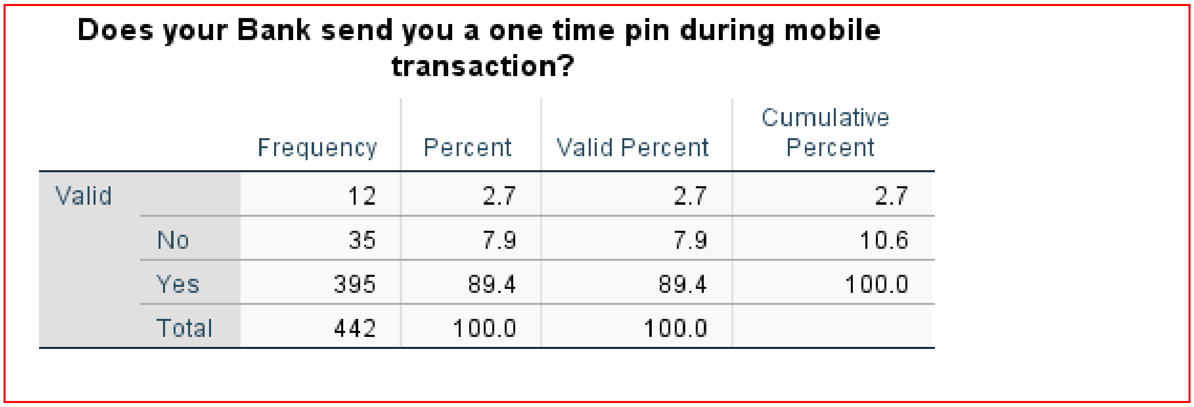


Do you think using PIN alone to log in and do transactions is insecure?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	4	.9	.9	.9
	3	18	4.1	4.1	5.0
	4	112	25.3	25.3	30.3
	5	308	69.7	69.7	100.0
	Total	442	100.0	100.0	

Figure 9:Using PIN alone for transactions is Insecure

The figure below shows distribution and percentages of responses, if the respondents received OTP when doing transactions. **89.4%** receive OTP, **7.9%** did not receive OPT while **12%** did not respond.

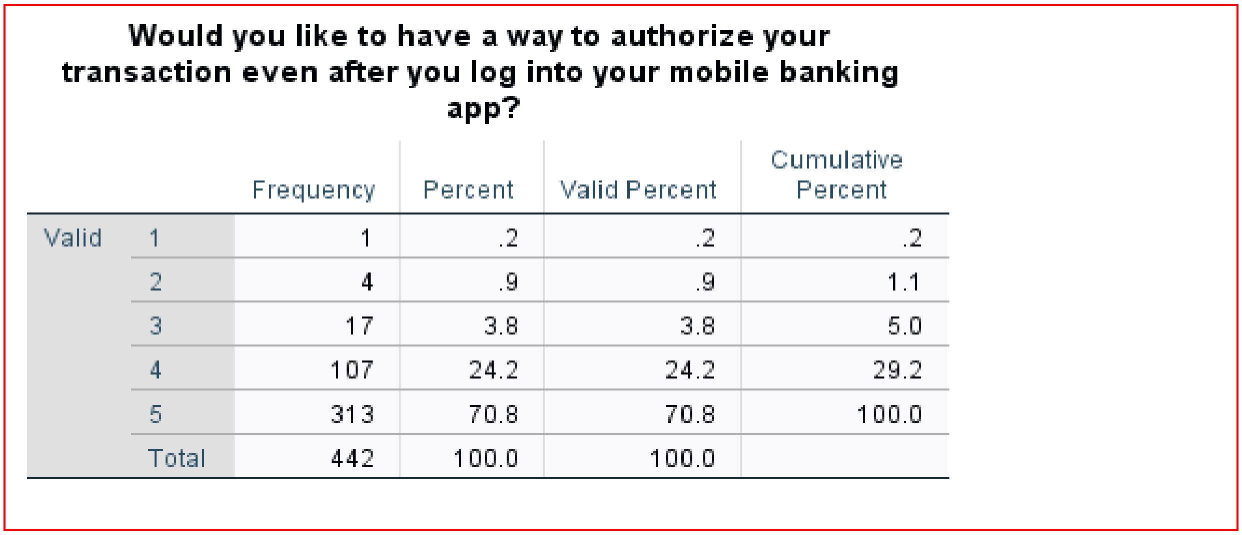


Does your Bank send you a one time pin during mobile transaction?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		12	2.7	2.7	2.7
	No	35	7.9	7.9	10.6
	Yes	395	89.4	89.4	100.0
	Total	442	100.0	100.0	

Figure 10: Respondents who receive OTP during Transactions

The figure below shows statistical responses on the respondents' willingness to recommend to their bank, a need to authorized transactions even after login. **70.8%** Strongly Agreed, **24.2%** Agreed, **3.8%** were neutral. On the other hand, **0.9%** disagreed while **0.2%** Strongly Disagreed.

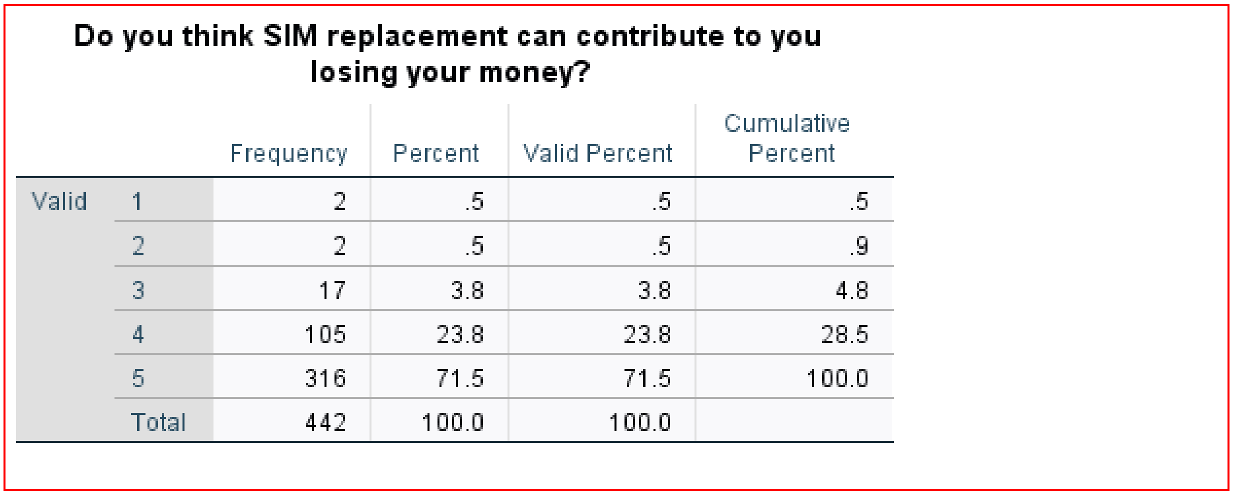


Would you like to have a way to authorize your transaction even after you log into your mobile banking app?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	.2	.2	.2
	2	4	.9	.9	1.1
	3	17	3.8	3.8	5.0
	4	107	24.2	24.2	29.2
	5	313	70.8	70.8	100.0
	Total	442	100.0	100.0	

Figure 11: Recommend a need for additional Authentication Mechanism to Banks

The figure below shows distribution and percentages of responses, if the respondents agreed with SIM Swaps to cause loss of money by customers. **71.5%** Strongly Agreed, **23.8%** Agreed, **3.8%** were neutral. On the other hand, **0.5%** disagreed while **0.5%** Strongly Disagreed.

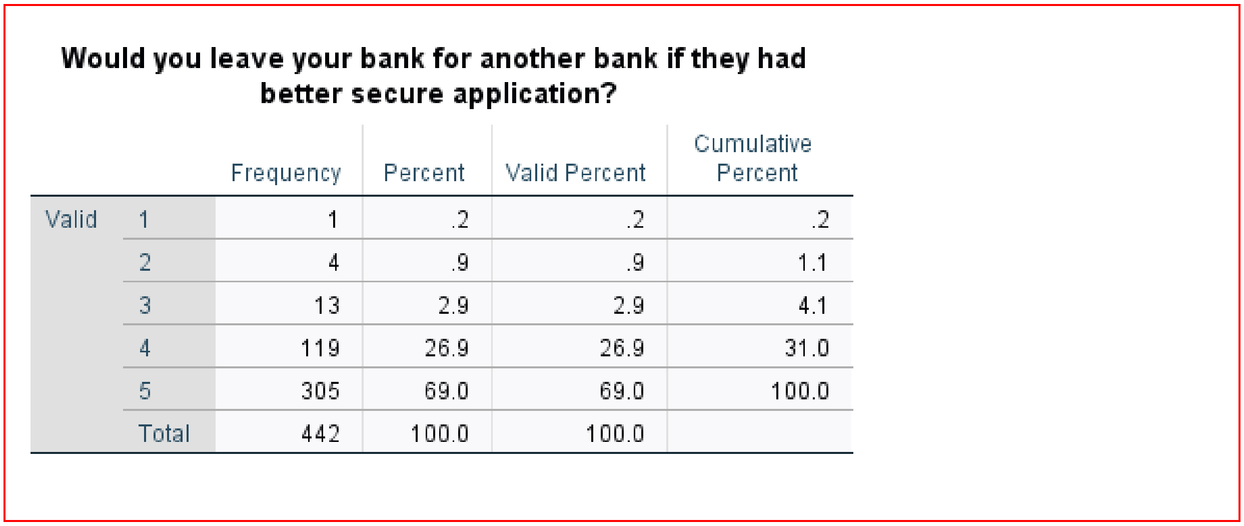


Do you think SIM replacement can contribute to you losing your money?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	.5	.5	.5
	2	2	.5	.5	.9
	3	17	3.8	3.8	4.8
	4	105	23.8	23.8	28.5
	5	316	71.5	71.5	100.0
	Total	442	100.0	100.0	

Figure 12:Sim swaps contribute to loss of money by customers

The figure below shows distribution and percentages of responses, if the respondents agreed to leave their current banks for another with a better secure mobile app. **69%** Strongly Agreed, **26.9%** Agreed, **2.9%** were neutral. On the other hand, **0.9%** disagreed while **0.2%** Strongly Disagreed.

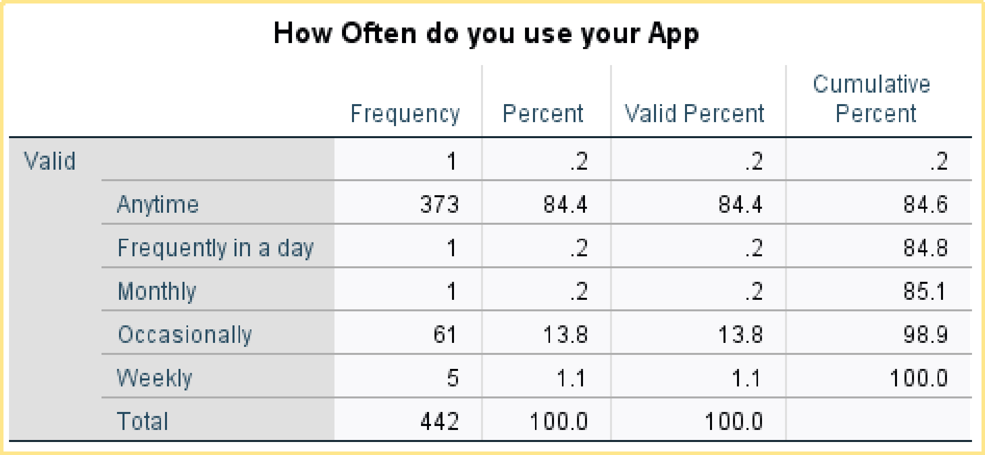


Would you leave your bank for another bank if they had better secure application?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	.2	.2	.2
	2	4	.9	.9	1.1
	3	13	2.9	2.9	4.1
	4	119	26.9	26.9	31.0
	5	305	69.0	69.0	100.0
	Total	442	100.0	100.0	

Figure 13: Customers loyalty change due to mobile banking security

The figure below shows distribution and percentages of responses on how often they use mobile banking. **84.4%** use mobile banking anytime of the day. Only **13.8%** use mobile banking occasionally while just **1.1%** use mobile banking on a weekly basis.



How Often do you use your App

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	.2	.2	.2
	Anytime	373	84.4	84.4	84.6
	Frequently in a day	1	.2	.2	84.8
	Monthly	1	.2	.2	85.1
	Occasionally	61	13.8	13.8	98.9
	Weekly	5	1.1	1.1	100.0
	Total	442	100.0	100.0	

Figure 14: Mobile baking usage

4.3 DESIGN

The design of the System involved the use of the following tools;

MS VISIO for the architectural components and Sequence diagrams. The following tools were then used to develop the prototype and also in the prototype's implementations.

Tool	Usage
InteliJ IDE	REST APIs development
Android Studio	Mobile Application Development
Azure Cloud Solution	• MySQL • Web App Service • Key Store • Azure DevOps-CI/CD
NodeJS, CSS, HTML5	Front end: Web User Dashboard
Third Party Systems	• SMS Gateway • USSD Push Gateway • HLR Database

Table 4: List of tools used in the USSD push Implementation

4.3.1 Database Design

MySQL was used to design and implement the database of Wybosoft Bank Limited. Figure 15 shows the Entity Relationship Diagram that displays the relational objects in the Wybosoft database.

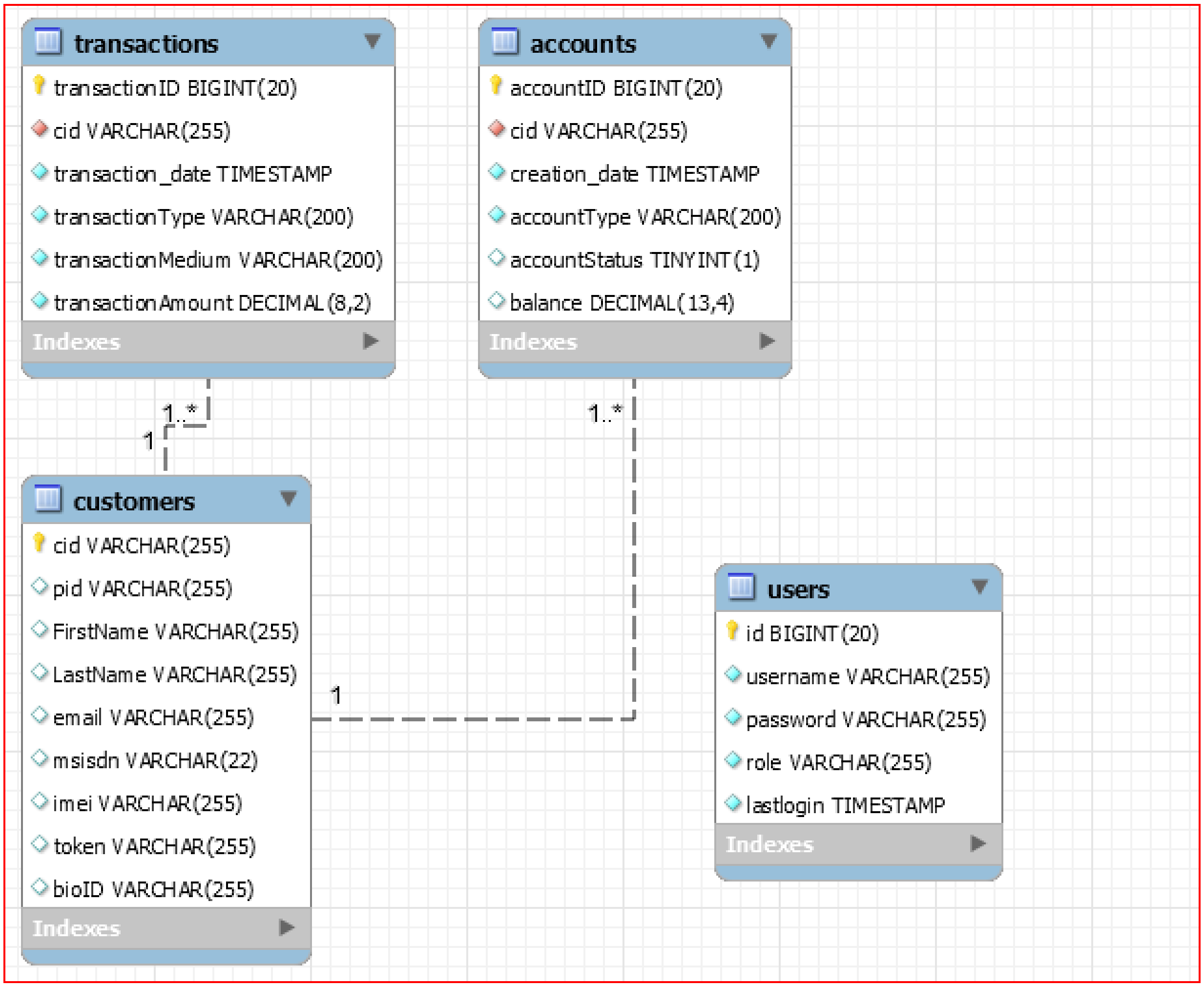


Figure 15: Shows ERD of Relations in the database

4.3.2 System Architecture

The system comprised of a set of components operated in distributed environment. The components are shown below.

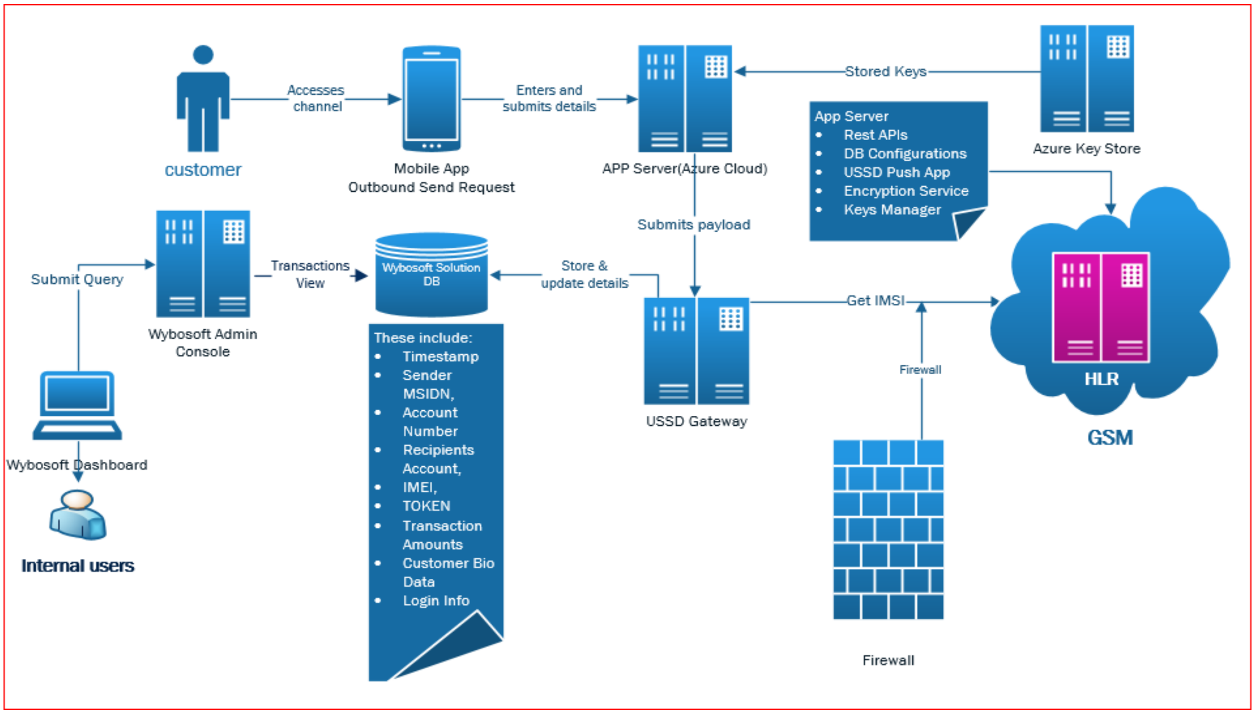


Figure 16: Wybosoft System Components

In the above figure, the components interacted as follows;

- App server. This component hosts all the rest APIs used in the project. It handles the application logic: Authentication for PIN, sends request for Certificate validation from Azure Key store. In addition, it forwards request for USSD push.
- Azure Key Vault/Store-Validates the certificate use by the application to adhere to Public Key Cryptography Standards
- USSD Gateway-This component ensure MFA by generating a ussd Push to the Device with a specified IMEI, IMSI, Device ID and MSISDN in the payload from APP Server.
- GSM-HLR- Assist in the retrieval of IMSI based on the mobile phone Number. It also ensures that SMS notification are sent to MSISDN doing transaction and also recipient.
- Wybosoft Database. This component has the database schema and the information stored in the database.
- Wybosoft Admin Console. This component runs on azure app server and provides the integration point between the Wybosoft Dashboard and the REST APIs leading to connection to the Wybosoft database.

- Wybosoft Dashboard-Allows the User to view database contents.
- Firewall-Provides traffic filtering between the GSM and USSD gateway.

CHAPTER 5 RESULTS AND DISCUSSIONS

5.1 Survey Results

The information was analyzed based on different questions from diverse respondents gave several insights. It is evident from study that mobile banking is part of daily lives of most bank's customers. This is evident on the number of respondents who use mobile banking daily being 84.4%. They use mobile banking anytime of the day. Only 13.8% use mobile banking occasionally while just 1.1% use mobile banking weekly. These descriptive statistics on frequent usage of mobile banking provides conducive environment for malicious individuals to fraud Kenyans of their hard-earned money. Therefore, mobile banking applications always need to be more secure to offer security.

The other finding was that the de-facto login method used by mobile banking applications in Kenya, is via PIN. This is depicted by 98% of the responses from 14 banks representing the target population size. Therefore, it can be concluded that mobile banking challenges have been largely contributed by using as the only factor of authentication. 69% of respondents have incurred losses due to compromised PINs. Hence there is a need for multi factor authentication.

Closely related to using PIN alone as the only authentication and authorization mechanism is the anonymous and sometimes known users' login into system to do unauthorized transactions on behalf of customers. This was evident on the 73.3% of respondents strongly agreed and 23.1% agreed that some losses have been caused by individuals. Therefore, there is a need to prevent such users from carrying out such transaction by implementing a sure way of ensuring authentication and authorization as documented in ISO/IEC 27000:2018 including confidentiality.

The next mobile banking challenges that came out is sim swap fraud. Several respondents agreed that sim swap had led to losses by mobile banking customers. A total of 71.5% of the respondents strongly agreed that swaps can make customers incur losses. With a 23.8% agreeing on the same, it was concluded that a secure system prone to this kind of challenge should be developed hence USSD push. In the case of swaps, USSD push ensures that every mobile transaction is authenticated for MSISDN, IMEI and IMSI. These pieces of information are acquired during registration hence if a sim-swap is done, the IMSI would have changed and the hash value of existing token made up of device ID and IMEI would be different. This would make all transactions initiated from a swapped sim card to fail.

Most respondents agreed with the need of an additional layer or mechanism to authorize/authenticate transaction even when a mobile banking user had been successfully logged in. 70.8% strongly agreed and a further 24.2% agreed on then need to have another layer of authentication. This formed another strong foundation for the development of a prototype to assist in mitigating the risk associated with mobile banking hence USSD push as MFA mechanism.

Consequently, 69% of the respondents strongly approved that they would leave their current bank for another bank if they offered a more secure mobile banking services and a further 26.9% agreed on the same. This provided a significant backing for the implementation of a prototype that can be used to demonstrate to financial intuitions that they can increase customer loyalty of they had better and secure mobile banking services.

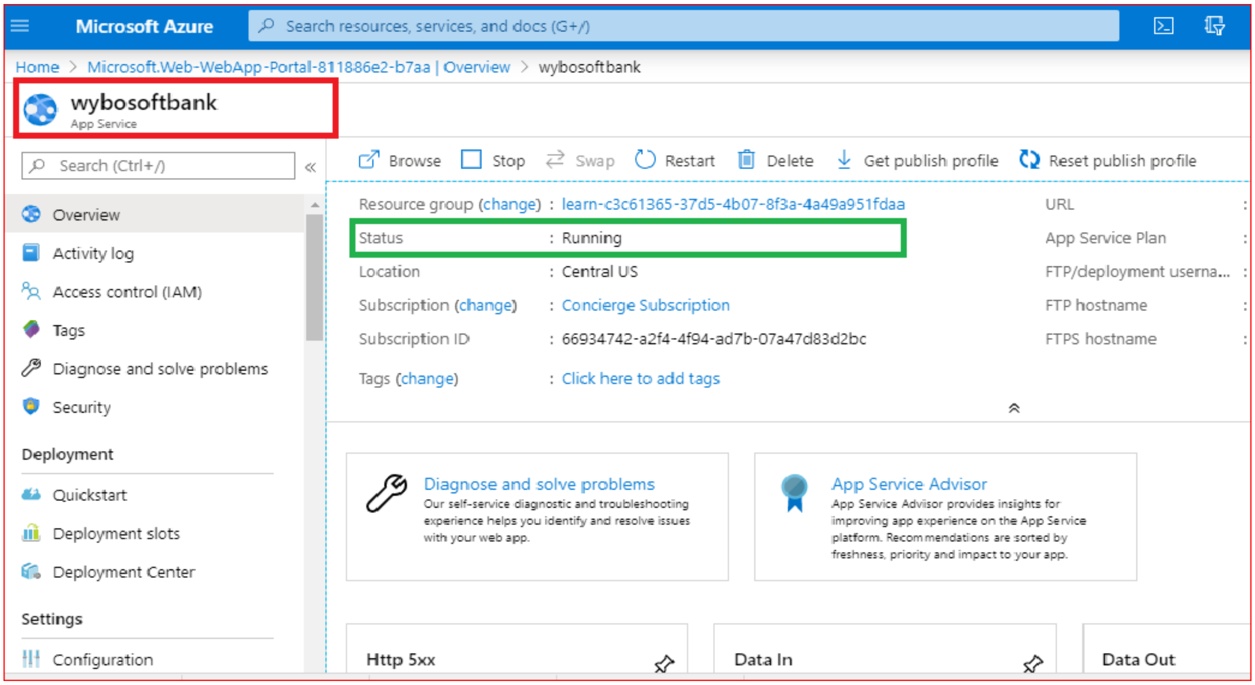
Using SWOT analysis method data collected, the researcher used outcome of the survey descriptive numerical values to indicate weaknesses, opportunities and threats of an of the authentication method in use right now by banks in Kenya. This in turn provided a holistic picture about the problem under study. This method helped to create effective and a valid basis on which a prototype to mitigate the mobile banking challenges identified was developed. In addition, the findings helped achieve the objective of the study which was to determine the need of an additional layer of security in mobile banking transactions.

Furthermore, the results of the survey assisted immensely in answering the research question on the security challenges in mobile banking transactions as a result of using PIN as the only factor of authentication and authorization. From the results, it is apparent that using PIN has led to losses by mobile Banking customers. The other challenge that was determined was the issue with Sim Swaps. All these were findings after the analysis of the data collected which confirms the problem which was to be addressed by this study.

In conclusion, the above results of the survey and discussion laid bare a need to develop a system that can mitigate the highlighted risks faced by mobile banking customers in Kenya. The resulting discussion let to the development of a system (Prototype), hereafter referred to as Wybosoft Bank System, whose implementation is discussed in the next section.

5.2 The Prototype

The System was developed under a fictional name of Wybosoft Bank. Wybosoft always offers a mobile-banking app to allow its customers to access their online banking services. That convenience and comfortable banking at hand as whenever need arises there by changing the narrative of brick and motor banking to something people do. The REST web services re hosted on Azure Cloud Service.



Resource group (change) : learn-c3c61365-37d5-4b07-8f3a-4a49a951fdaa
Status : Running
Location : Central US
Subscription (change) : Concierge Subscription
Subscription ID : 66934742-a2f4-4f94-ad7b-07a47d83d2bc
Tags (change) : Click here to add tags

URL :
App Service Plan :
FTP/deployment userna... :
FTP hostname :
FTPS hostname :

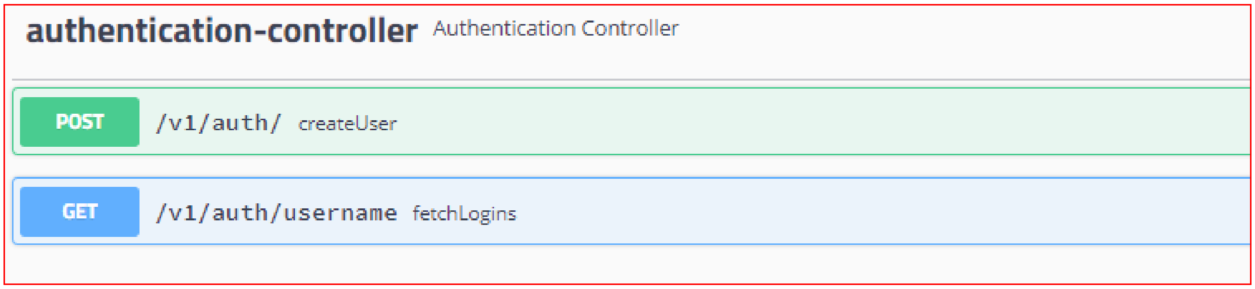
Diagnose and solve problems
Our self-service diagnostic and troubleshooting experience helps you identify and resolve issues with your web app.

App Service Advisor
App Service Advisor provides insights for improving app experience on the App Service platform. Recommendations are sorted by freshness, priority and impact to your app.

Figure 17: Azure Cloud solution in running state

5.2.1 The APIS

The figure below show sample API as documented in Swagger API services. A number of APIs were developed to be consumed by both Mobile Banking App and the dashboard to achieve the actual implementation of the entire project.



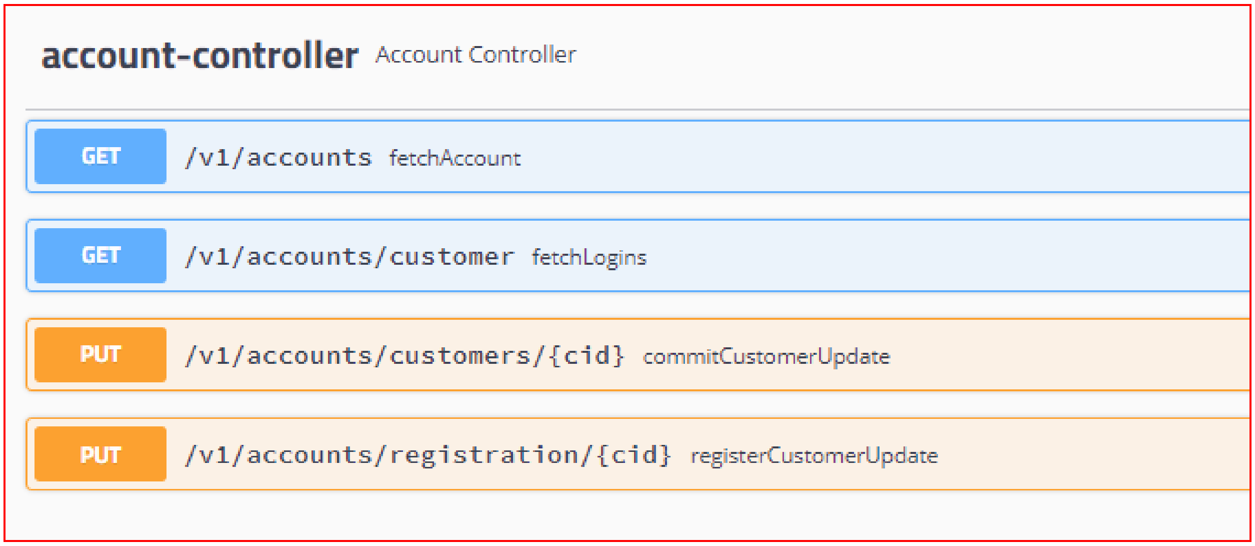
authentication-controller Authentication Controller

POST /v1/auth/ createUser

GET /v1/auth/username fetchLogins

Figure 18: Showing Login APIs

The figure above shows list of APIs used to authenticate users on the Web application. The APIs also handled Pin authentication methods on the Wybosoft Mobile Banking App.



account-controller Account Controller

GET `/v1/accounts` fetchAccount

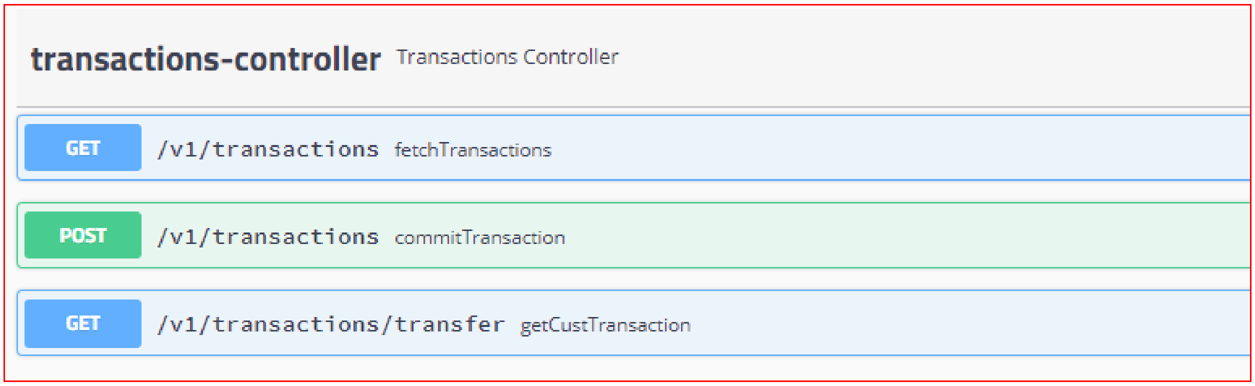
GET `/v1/accounts/customer` fetchLogins

PUT `/v1/accounts/customers/{cid}` commitCustomerUpdate

PUT `/v1/accounts/registration/{cid}` registerCustomerUpdate

Figure 19: Showing Accounts APIS

The figure above shows the list of APIs that were used to handle all account based REST request.



transactions-controller Transactions Controller

GET `/v1/transactions` fetchTransactions

POST `/v1/transactions` commitTransaction

GET `/v1/transactions/transfer` getCustTransaction

Figure 20: Shows APIs for transaction

The figure above shows a list APIs that were used to handle all transaction from the Wybosoft Mobile Banking App.

5.2.2 Why REST APIs.

Modern application designs yarn to achieve a given set of objectives that revolves around distributed architectures.

In the design of the project implantation, we chose the REST API architecture over SOAP because of ease of design, development, testing and implementation. REST architecture delivers greater performance, predominantly through caching for information that’s unchanged and static as documented in (Stackify, 2020).

During the design the following distributed systems principles were considered.;

- **High Availability**-This was ensured by provisioning Load Balancer in the Azure cloud service. Such that one node running the App server goes down, the other is able to pick and continue the operations.
- **Security**-Azure Key Vault enabled the secure access of stored secrets which is the core reason for the undertaking of the project in the first place.
- **Efficiency**-Rest architecture are known to be light and therefore consume less bandwidth and operates asynchronously. Hence resources are not tied until a given operation is complete due to blocking-wait protocol.
- **Scalability**. Azure Fault Domain helps in ensuring that instances are automatically added as per the demand of the systems utilization. This is known as **scale out (Horizontal scaling)**. For instance, as number of Wybosoft mobile Banking users increase, azure would ensure that compute resources are added to handle the spike in traffic (Azure, 2020).

5.2.3 Registration

When the a Wybosoft bank customer wants to register for mobile baking, they are prompted to key in their details. This is based on a condition that they must be having an active account already with the bank.

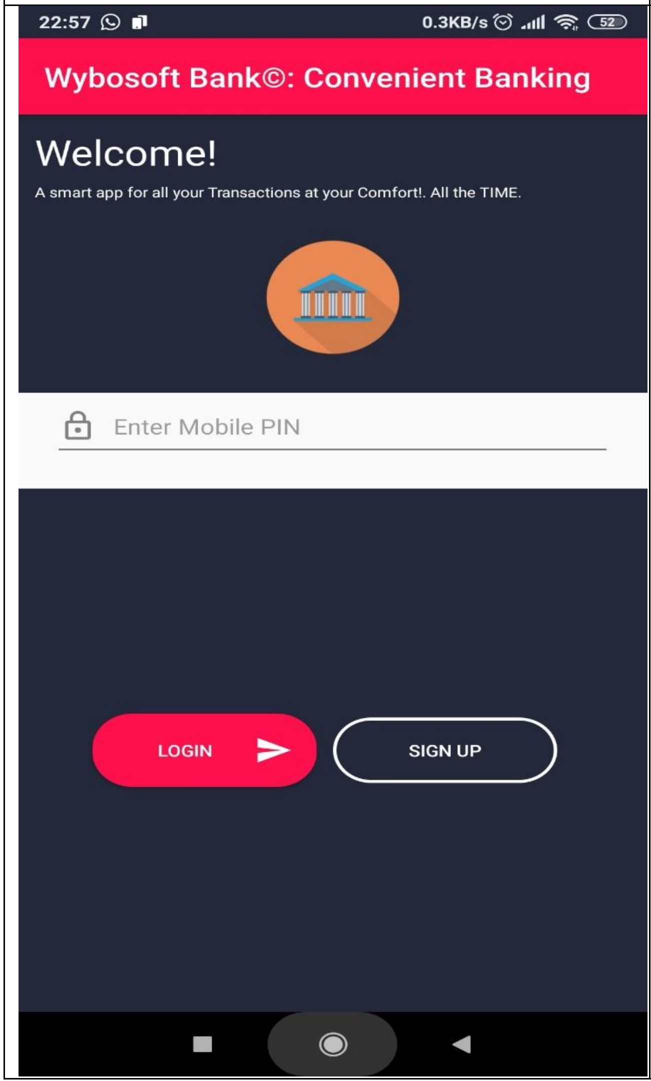
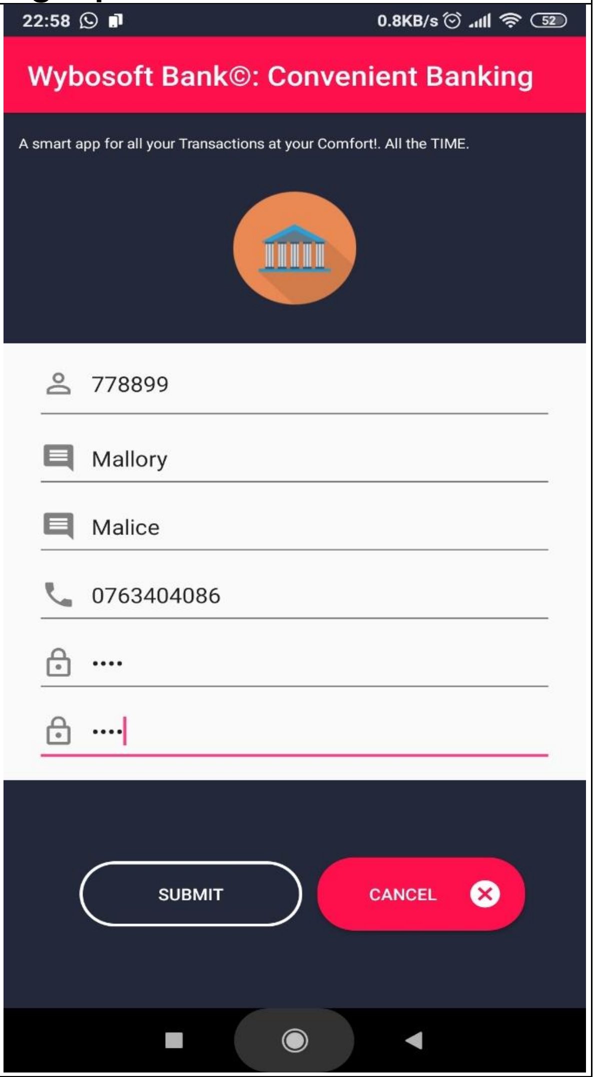
First Screen	Signup Screen
 Wybosoft Bank©: Convenient Banking Welcome! A smart app for all your Transactions at your Comfort!. All the TIME. Enter Mobile PIN 	 Wybosoft Bank©: Convenient Banking A smart app for all your Transactions at your Comfort!. All the TIME. 778899 Mallory Malice 0763404086 ···· ····

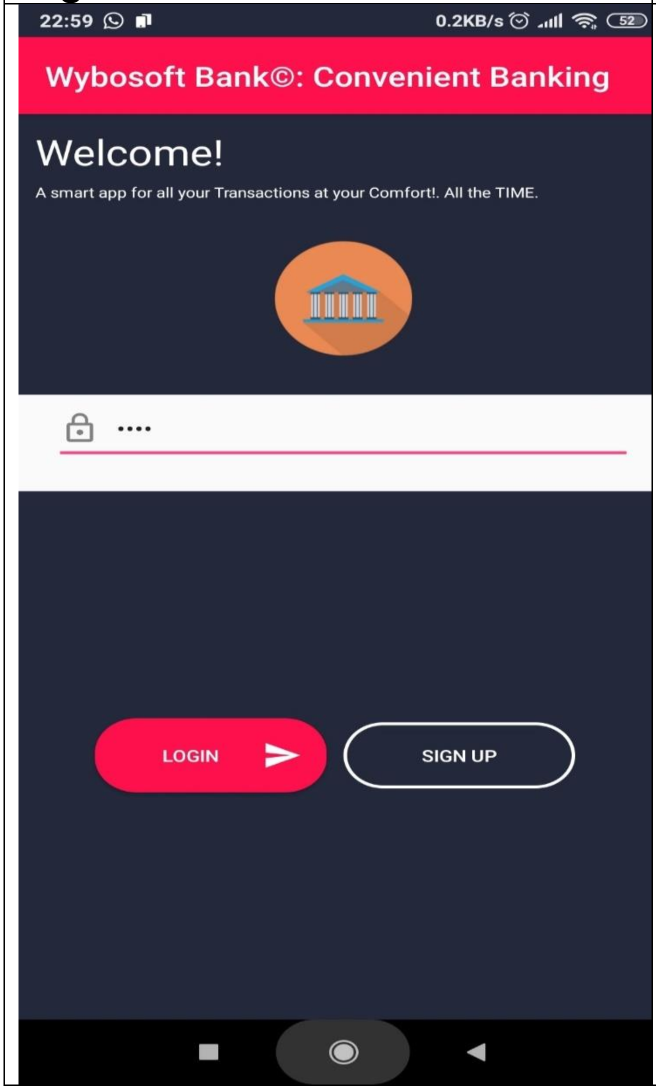
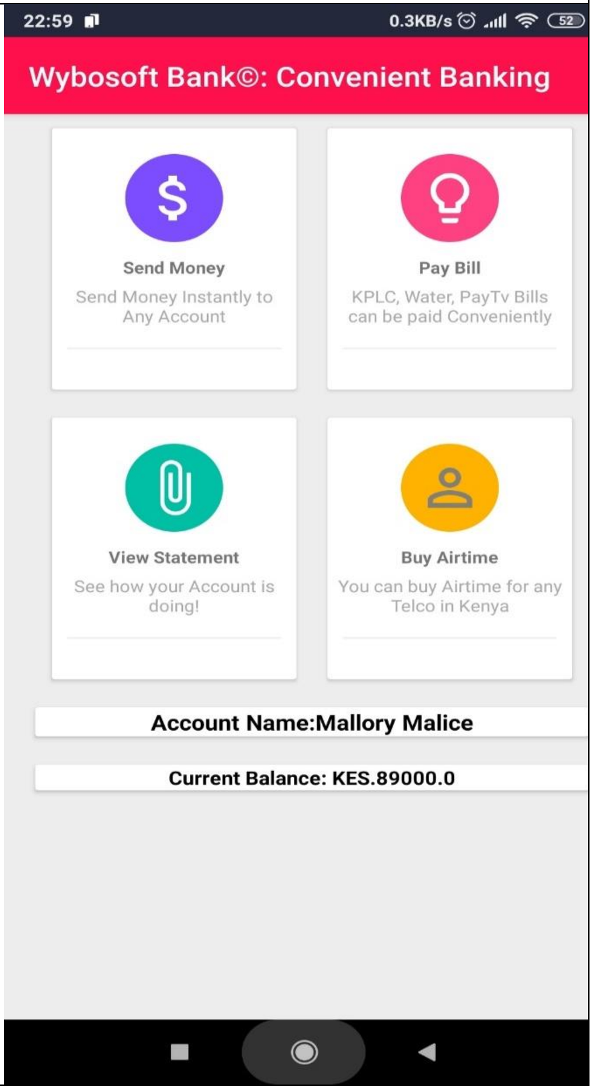
Table 5: Shows Login and Signup Screens respectively

Once the details have been keyed in correctly, the mobile banking application obtains device ID, IMEI and generated a token. All these details: Account, First Name, Last Name, Phone Number and Confirmed PIN leave the device in an encrypted format. The encryption is done by Bcrypt algorithm. This adheres to OWASP guidelines for data in transit security.

The data is then forwarded by the REST web service, running on Azure Cloud service, to the database running on MySQL also on Azure Cloud. The data saved there is also encrypted for PIN field. This also adheres to OWASP guidelines for data at rest.

5.2.4 Login

Upon successful registration, the user is prompted to login with the chosen pin during registration. The login screen is shown below. Note that challenge associated with PIN delivery is mitigated by not sending a customer a login PIN but instead they chose it themselves. After successful login, the customer is presented with a home screen as shown below.

Login Screen	Home Screen
	

22:59
0.2KB/s
Wybosoft Bank©: Convenient Banking
LOGIN
SIGN UP

Welcome!

A smart app for all your Transactions at your Comfort!. All the TIME.

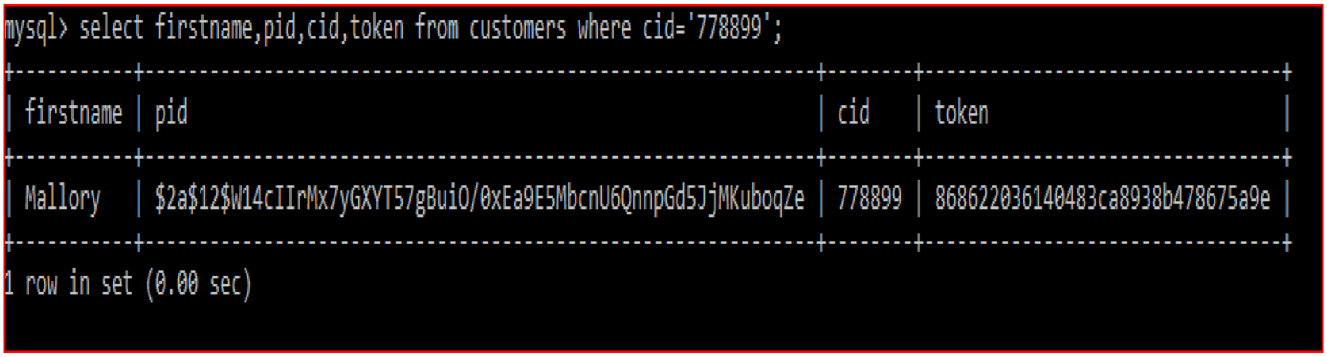
22:59
0.3KB/s
Wybosoft Bank©: Convenient Banking
Send Money
Send Money Instantly to Any Account
Pay Bill
KPLC, Water, PayTv Bills can be paid Conveniently
View Statement
See how your Account is doing!
Buy Airtime
You can buy Airtime for any Telco in Kenya

Account Name:Mallory Malice

Current Balance: KES.89000.0

Table 6: Shows Login Screen and Home Screen Respectively

NB: The PIN is stored in an encrypted format as shown below. Also note the token as a concatenation of IMEI and Device ID. The customer PIN is a combination of four digits. But the Bcrypt encryption has made it a string of characters. This adheres to InfoSec requirement for storage of sensitive data.



```
mysql> select firstname,pid,cid,token from customers where cid='778899';
+-----------+--------------------------------------------------------------+--------+---------------------------------+
| firstname | pid                                                          | cid    | token                           |
+-----------+--------------------------------------------------------------+--------+---------------------------------+
| Mallory   | $2a$12$W14cIIrMx7yGXYT57gBuiO/0xEa9E5MbcnU6QnnpGd5JjMKuboqZe | 778899 | 868622036140483ca8938b478675a9e |
+-----------+--------------------------------------------------------------+--------+---------------------------------+
1 row in set (0.00 sec)
```

Table 7: Show encrypted information in Customer relation, Wybosoft Database

The token is used to authenticate the user when they initiate a transaction such as send money. We will see this shortly.

5.2.5 Transaction

Whenever a user initiates a transaction such as send money, the request is submitted from the handset to the application server in an encrypted format. Once user's PIN is authenticated successfully, second factor of authentication is done using the IMEI and Device ID obtained from the database. The recipient First Name and Last Name is also retrieved to be displayed.

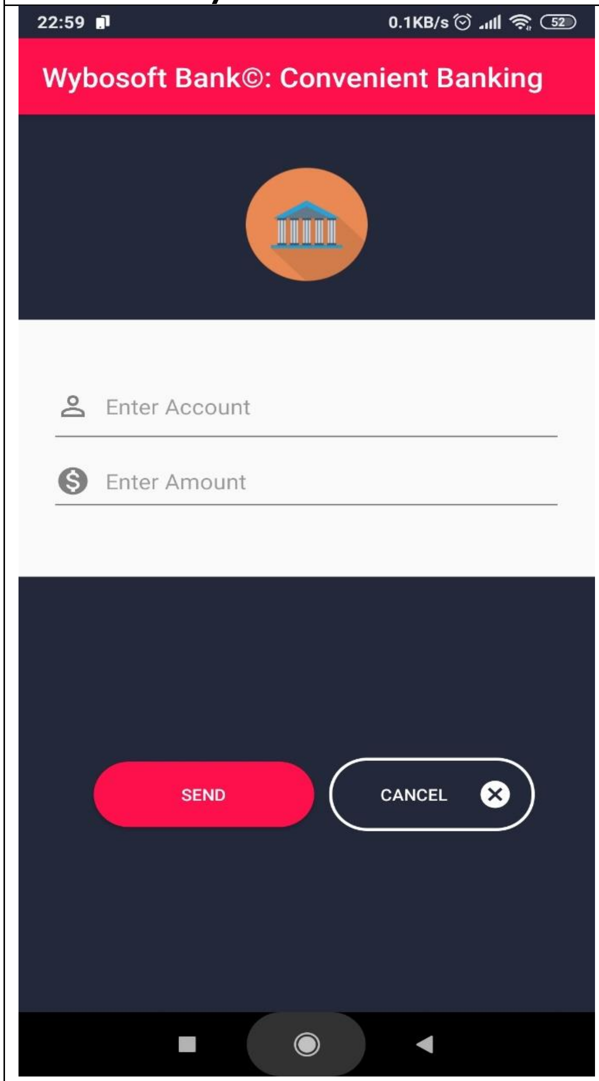
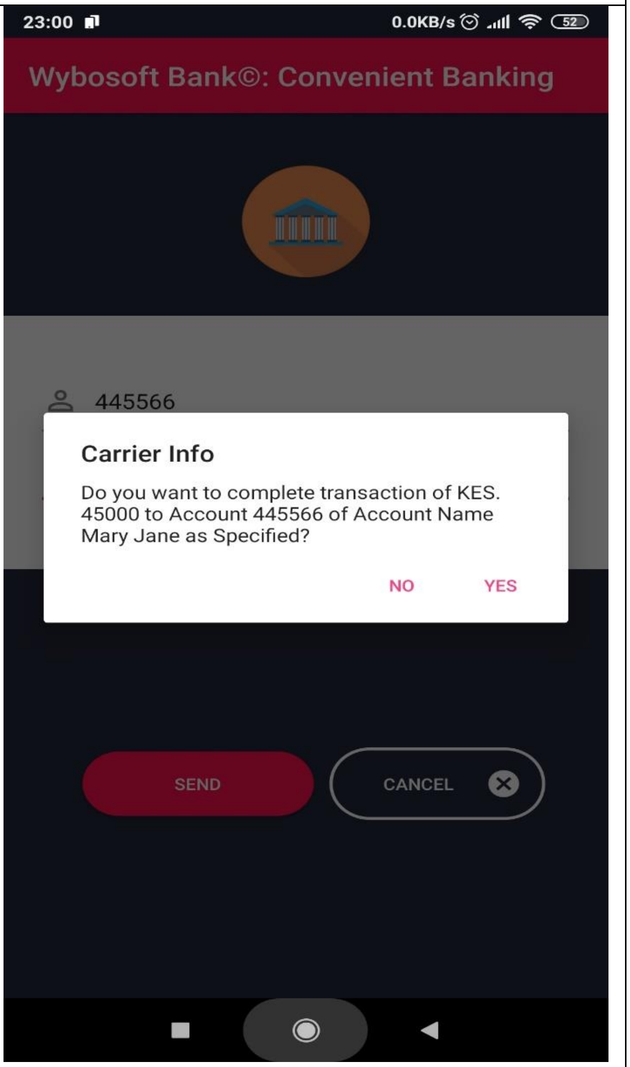
The data flow is also encrypted. This is ensured by secure socket layer(SSL). The rest service then forwards the request to USSD gateway which process the request based on the token and MSISDN. The MSISDN is compared again a GSM database called HLR for IMSI which was there previously. If this is correct, then the third authentication factor is done of the device that instated the transaction. A USSD push is send to the device with the device ID and IMEI base on IMSI associated with MSISDN.

User is then asked if they wish to complete the transaction for the given details as specified.

Customer can:

- Choose to cancel transaction if they didn't initiate it. This is in case of a sim swap which is very unlikely since IMSI would differ and so IMEI and also device ID.
- Accept and Authorize transaction if everything is successful.

Note the balance before USSD push is KES. 89000.

Send Money Screen	USSD Push Screen
	

Carrier Info

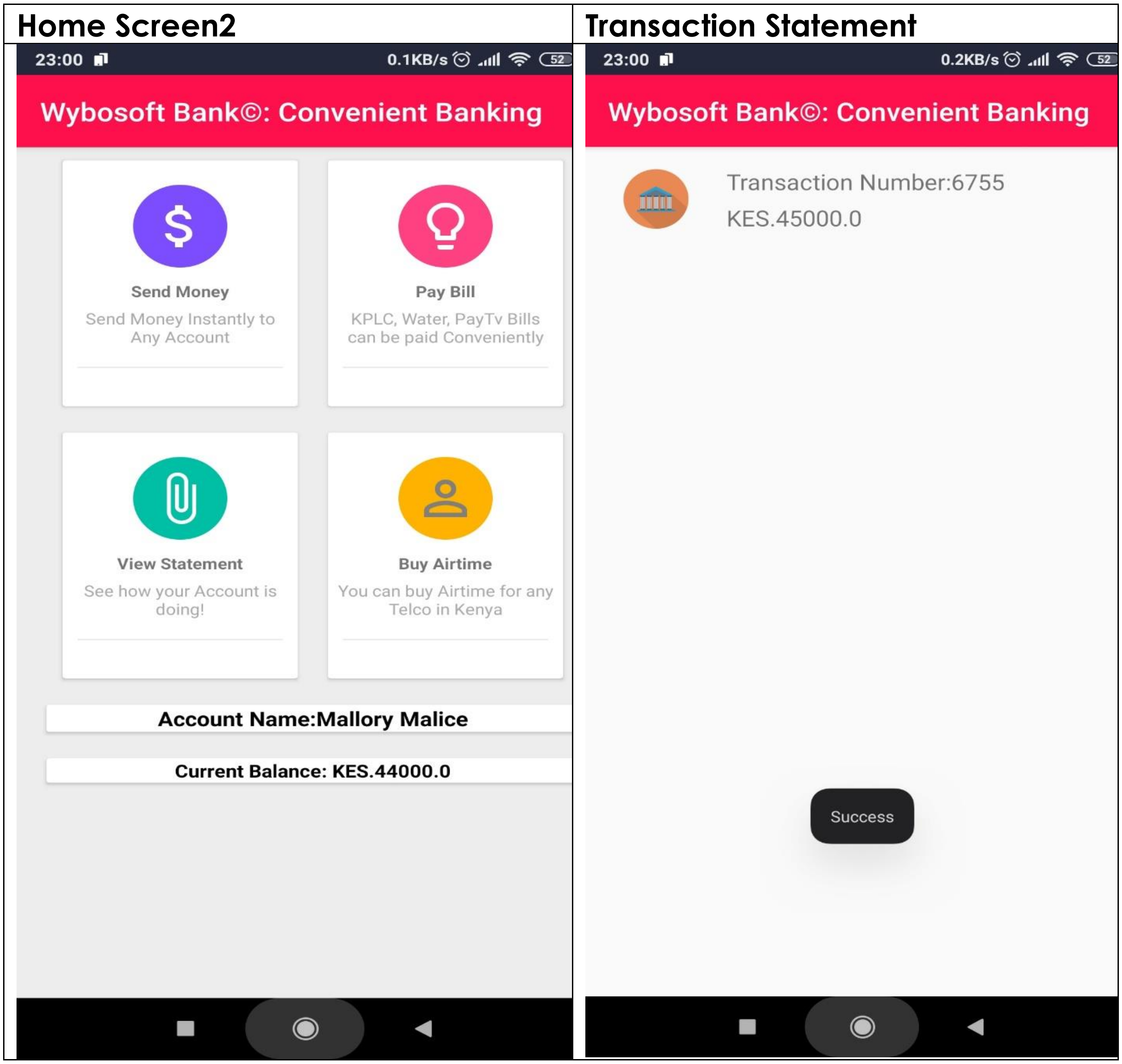
Do you want to complete transaction of KES. 45000 to Account 445566 of Account Name Mary Jane as Specified?

NO YES

Figure 21: USSD push to customer via the App

Notice on the USSD push come with header carrier info. This indicates that the data is independent of the channel used to initiate the transaction.

If the user chooses yes, the sender account is debited with an equivalent amount specified before USSD Push. See the next page for completed transaction and the statement.


Home Screen2
Transaction Statement
23:00
0.1KB/s
0.2KB/s
52
Wybosoft Bank©: Convenient Banking
Send Money
Send Money Instantly to Any Account
Pay Bill
KPLC, Water, PayTv Bills can be paid Conveniently
View Statement
See how your Account is doing!
Buy Airtime
You can buy Airtime for any Telco in Kenya
Success

Account Name:Mallory Malice

Current Balance: KES.44000.0

Transaction Number:6755

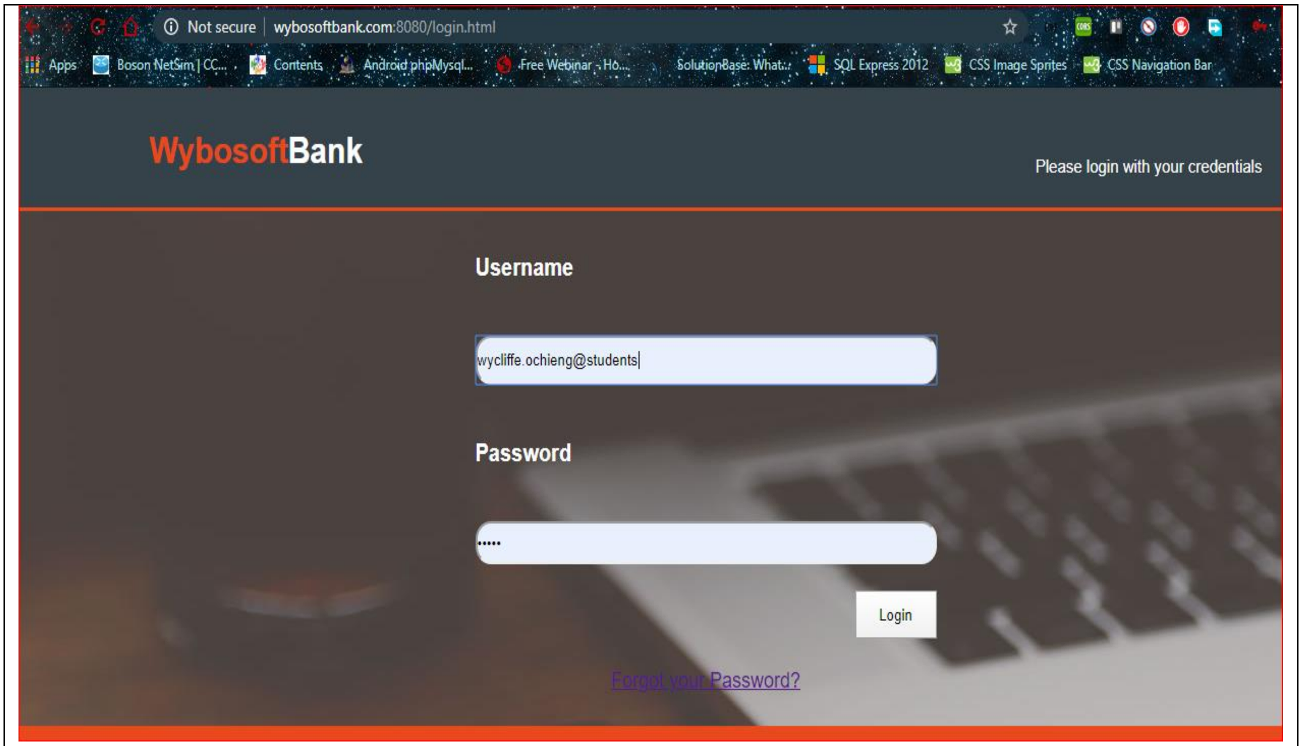
KES.45000.0

Figure 22: New transaction status with statement to the right

5.2.6 Wybosoft Dashboard

The bank has a dashbord that can be used to view trasancion and othera ccount details on limited view only. A bank user is expected to login with username and password. No user is capable of carrying out a areansacion of behanlf of a customer. Hence mitigating the outcome of the resarch that users can login into the system and carry out transactions. The dashboard is hown in the below. The dashboard is also running in wybosft Azure Cloud on custom domain www.wybosoft.com.

Bank User: Login Screen



Username

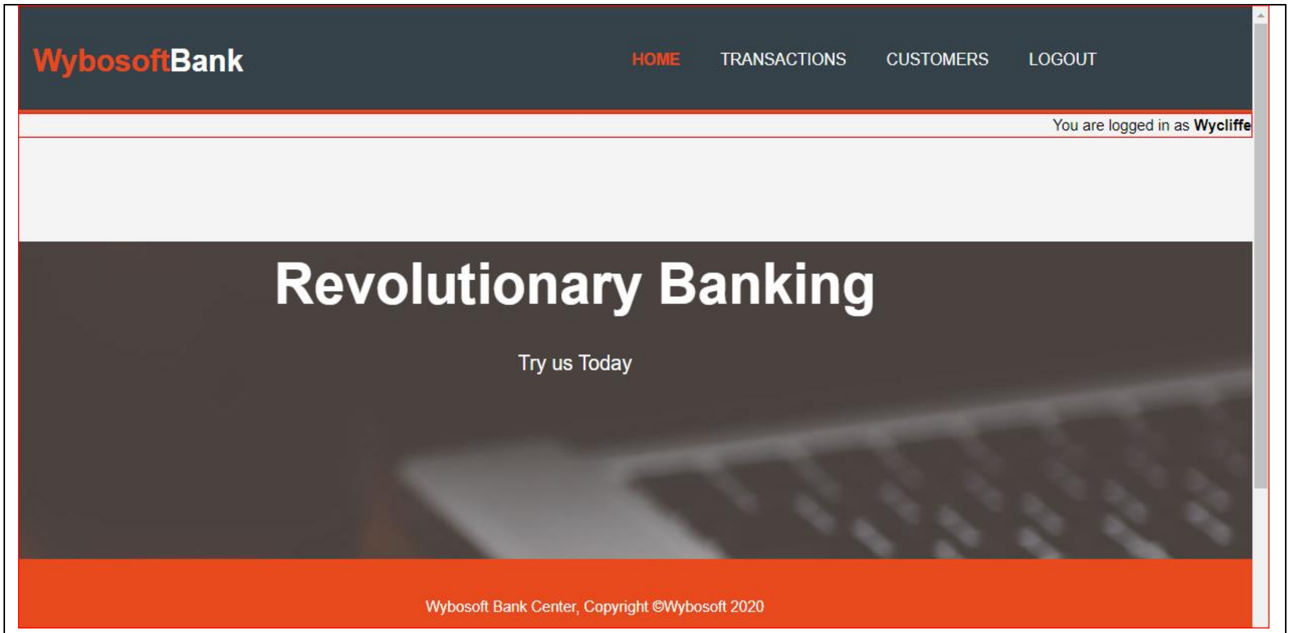
wycliffe.ochieng@students

Password

•••••

Figure 23: Dashboard Login

Bank User: Home



WybosoftBank

You are logged in as **Wycliffe**

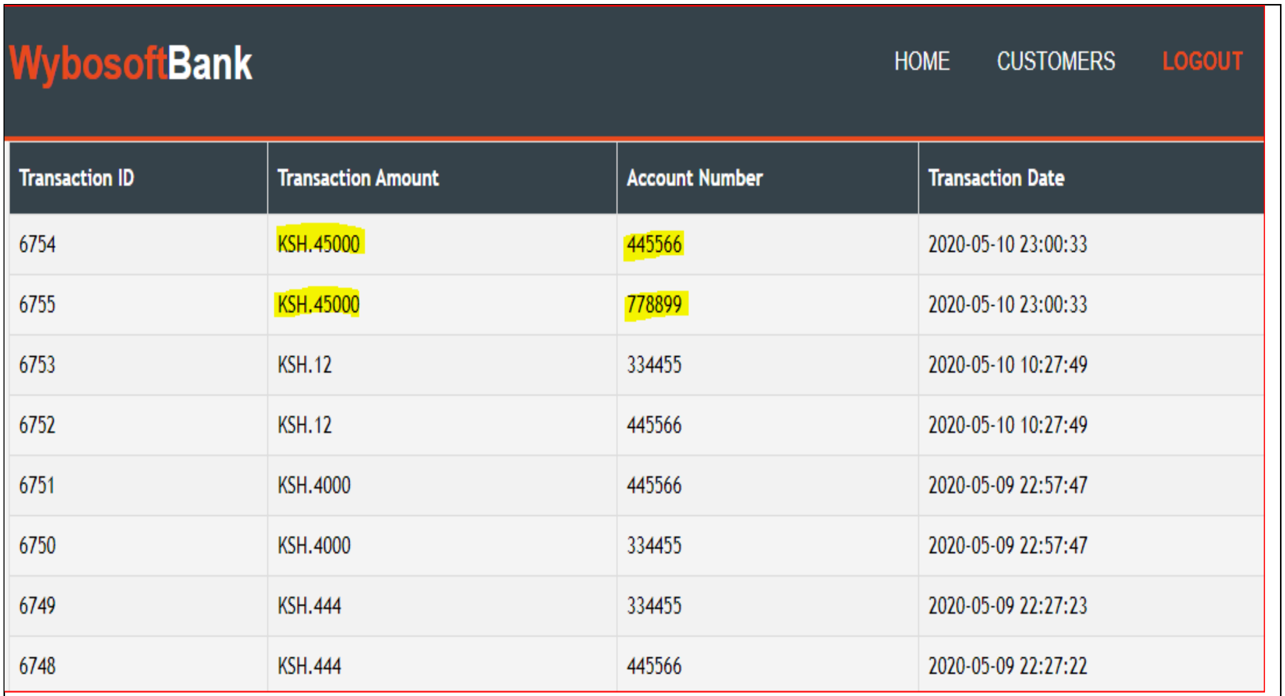
Revolutionary Banking

Try us Today

Wybosoft Bank Center, Copyright ©Wybosoft 2020

Figure 24: Dashboard Home

Bank User: Transactions



Transaction ID	Transaction Amount	Account Number	Transaction Date
6754	KSH.45000	445566	2020-05-10 23:00:33
6755	KSH.45000	778899	2020-05-10 23:00:33
6753	KSH.12	334455	2020-05-10 10:27:49
6752	KSH.12	445566	2020-05-10 10:27:49
6751	KSH.4000	445566	2020-05-09 22:57:47
6750	KSH.4000	334455	2020-05-09 22:57:47
6749	KSH.444	334455	2020-05-09 22:27:23
6748	KSH.444	445566	2020-05-09 22:27:22

Figure 25: Dashboard Transactions

5.2.7 Prototype Evaluation results

The Mobile Banking Application (.apk) file was shared by end users who had participated in the survey for evaluation. A sample questionnaire form used to gather feedback from the end users has been attached in appendix B.

A total of two hundred and ninety-six end users responded and distribution per and gender was as shown below. Figure 26 shows that 68.9%of responded are quite youthful land only 6.1% fall above youthful age. Therefore, mobile banking is more embraced by youths. From *Figure 28*, 46.6% or respondents were female while 53.4% were male.

Figure 29 illustrates the ratings of the USSD feature that was to meet the objective of the study. 69.9 Strongly liked the feature and 25.7% agreed with the feature. Only a 4.7% of the responded did not agree or disagree with the USSD feature. This clearly demonstrated and validated the need for enhanced mobile banking security. This can be interpreted that the new feature was in harmony with customer experience.

On the other hand, a total of 92.6% felt that they needed a biometric feature such as fingerprint to be added on to that Application to further enhance the mobile banking security. While 7.4% felt there is no need for an additional authentication as depicted in *Figure 30*.

Further to new features, a total of 61.5% strongly agreed that they would recommend the banking app to other users as shown in Figure 31. An additional 32.1% agreed to do the same. This was a clear indication that the need for enhanced security had been satisfied. The responses were as follows:

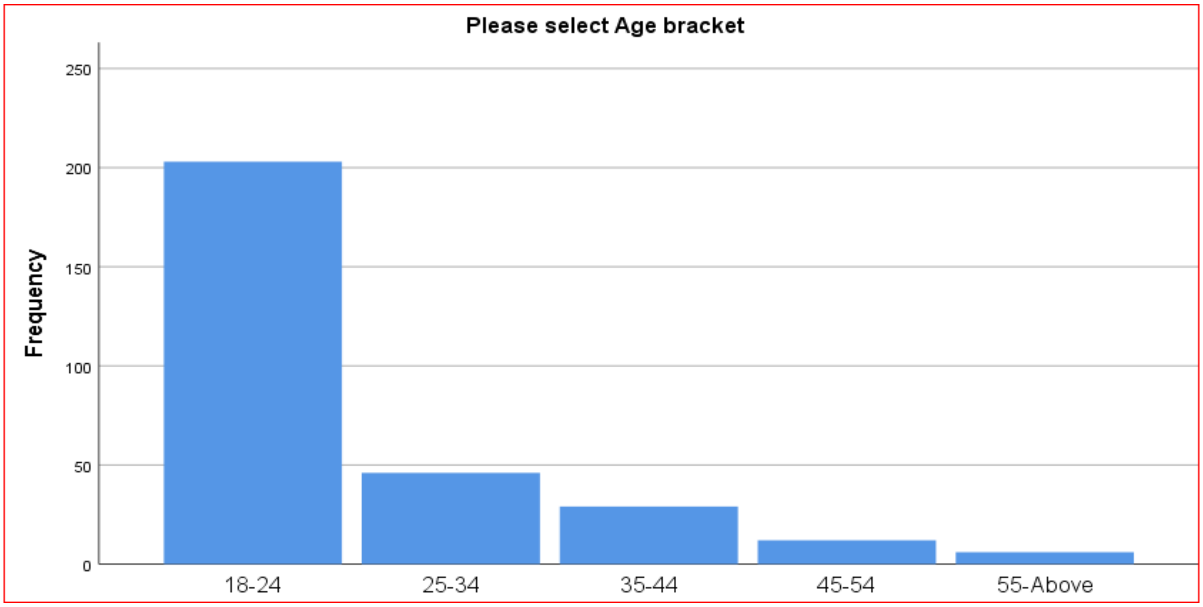
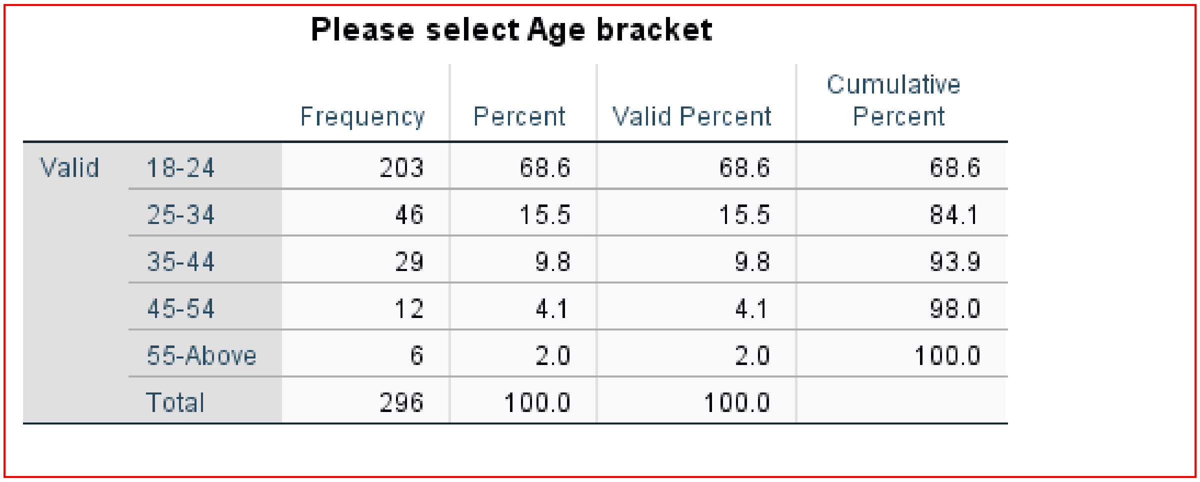


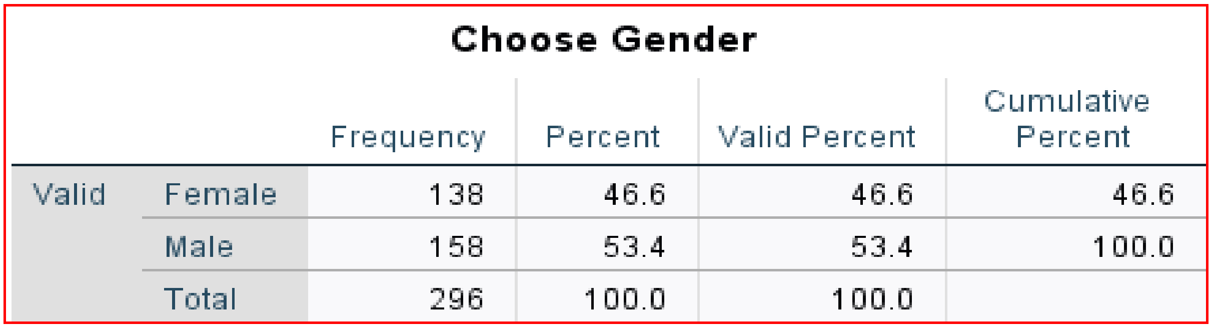
Figure 26: Bar graph showing Age distribution



Please select Age bracket

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-24	203	68.6	68.6	68.6
	25-34	46	15.5	15.5	84.1
	35-44	29	9.8	9.8	93.9
	45-54	12	4.1	4.1	98.0
	55-Above	6	2.0	2.0	100.0
	Total	296	100.0	100.0	

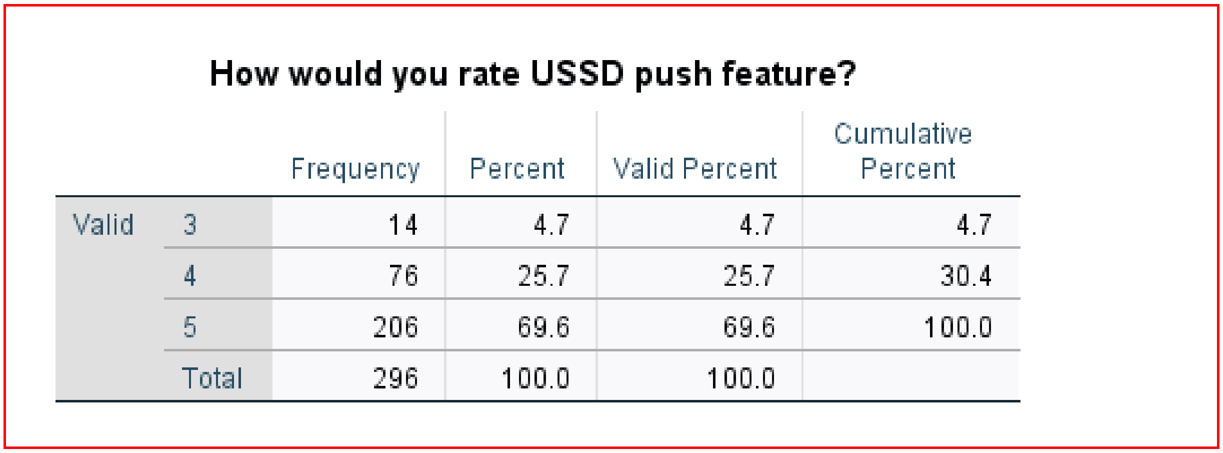
Figure 27: Descriptive distribution of prototype Evaluators



Choose Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	138	46.6	46.6	46.6
	Male	158	53.4	53.4	100.0
	Total	296	100.0	100.0	

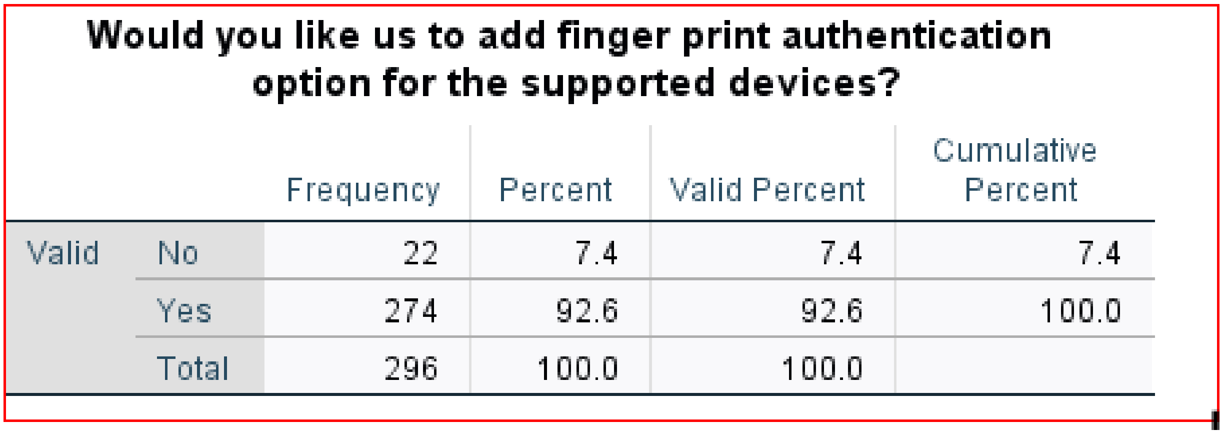
Figure 28: Gender Distribution



How would you rate USSD push feature?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	14	4.7	4.7	4.7
	4	76	25.7	25.7	30.4
	5	206	69.6	69.6	100.0
	Total	296	100.0	100.0	

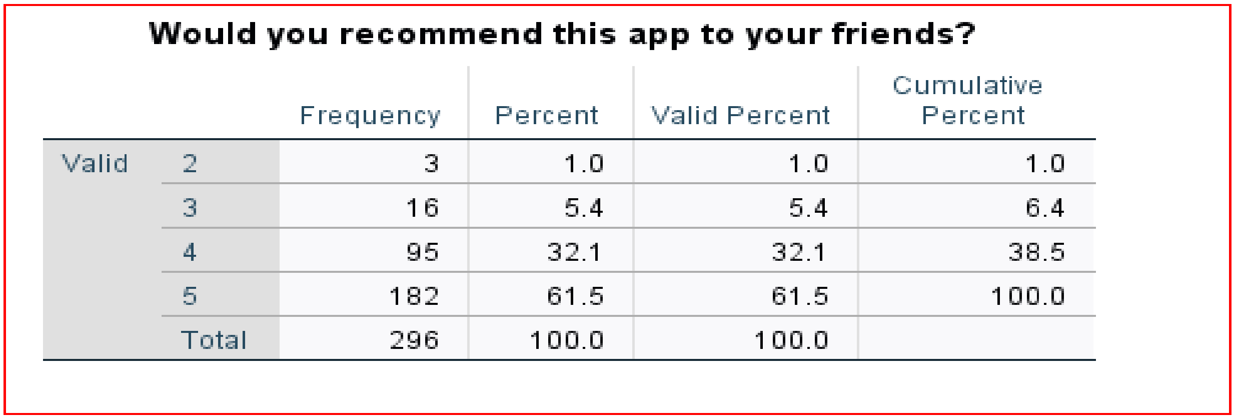
Figure 29: Ratings for USSD feature



Would you like us to add finger print authentication option for the supported devices?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	22	7.4	7.4	7.4
	Yes	274	92.6	92.6	100.0
	Total	296	100.0	100.0	

Figure 30: Recommendation for Biometric Feature



Would you recommend this app to your friends?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	3	1.0	1.0	1.0
	3	16	5.4	5.4	6.4
	4	95	32.1	32.1	38.5
	5	182	61.5	61.5	100.0
	Total	296	100.0	100.0	

Figure 31: Recommend the App to other Users

5.2.8 Prototype results and Discussions

The development and implement and implementation of the prototype provided a number of great insights about the study.

First, it helped in fulfilling the research objective of developing a mobile banking application prototype that demonstrate end to end secure mobile transactions. This was well executed by employing use of SSL and **BCrypt** Encryption Algorithm on the various components of the System. As shown, sensitive data at rest and in transit have were encrypted leading to a secure system. End to end secure transaction was also demonstrated by multifactor authentication via USSD push.

Secondly, the results from the prototype assisted in the evaluation of the effectiveness of incorporating a combined USSD push and PIN for a time efficient multifactor authentication. The application was quite responsive and with right infrastructure capacity, the system can work really effectively and efficiently.

On the other hand, the prototype helped in obtaining answers for the various research questions for this study. The study was to determine the alternative to the current mobile banking security models. The prototype provided solution to the research enquiry through demonstration of USSD architectures and subsequent implantations. It also assisted in demonstrating how USSD push could be used to enhance mobile banking security when implemented together with other factors of systems authentication such as Device ID, IMEI and IMSI.

In conclusion, the prototype provided conclusively a way of addressing highlighted mobile banking issues in chapter one of the report through the design and its implementation.

CHAPTER 6 CONCLUSION AND RECOMMENDATIONS

The research lead to development of a software product that demonstrated the objective highlighted in the research. The research has contributed to development of an authentication mechanism that utilizes an out of band GSM technology called USSD push. To this end, this has helped in achieving the research objectives: To develop a cost effective model that can be adopted by banks in Kenya. Thus a greatly reduced cost in offering secure mobile banking services since SMS using OTP is very expensive and unreliable. Secondly, if adopted by banks, it will help increased uptake e of mobile banking thereby leading to diverse revenue streams by banks in Kenya.

In addition, the research report also shows how the knowledge developed can be applied to related computer systems domain. Examples of such systems include single sign on remote user authentication over VPN or internet. Users can login into single sign on systems and be authorized once they complete a USSD push delivered to a pre-registered mobile phone number. This formed a basis for new system implementation paradigm. Therefore, a form of new knowledge.

6.1 Limitations

The project implementation faced several challenges. First data collection was based on sensitive information about banks customers. This was not easily availed by banks. The second challenge was securing an SMS gateway to assist in complete simulation of the SMS delivery part. Currently securing an SMS Gateway is quite expensive and needed some funding.

6.2 Further research and Recommendations

The concept investigated and implemented under this project is viable and can be undertaking further by carrying out research on how best authentication mechanisms can be implemented in various aspects of life

For instance, USSD push can be implemented on E-Commerce applications to allow authentication and authorization of uses doing online transaction and the push is sent to a mobile phone for completion of the payments.

Further research and studies can be done on areas around implication IRIS, fingerprint: Bio and even Artificial Intelligence (AI). The use of AI to establish customer transaction patterns to assist in curbing fraud by the system without human intervention. Should a malicious user get to genuine customers account using AI, the system is able to prevent the loss of funds before it takes place. These are possible areas of study that are not yet explored in terms of Mobile banking security. A lot more can be done.

REFERENCES

27000:2018, I., 2018. *ISO/IEC 27000:2018.* [Online]
Available at: https://www.iso.org/standard/73906.html
[Accessed 10 05 2020].

Adeoy, O. S., 2012. evaluating the performance of two-factor authentication solution in the banking sector. *International Journal of Computer Science Issues,* pp. 1-6.

Alhuseen O. Alsayed, A. L. B., 2017. E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities. *International Journal of Emerging Technology and Advanced Engineering,* pp. 1-8.

Anil K. Jain, P. F. A. R., 2008. *Handbook of Biometrics.* s.l.:Springer US.

Antal, M. & Szabó, L. Z., 2015. Biometric Authentication Based on Touchscreen Swipe Patterns. *Procedia Technology,* p. 862–869.

Associates, B. F., 2014. *MANAGING THE RISK OF MOBILE BANKING TECHNOLOGIES,* s.l.: FinMark Trust.

Azure, M., 2020. *Azure Autoscale.* [Online]
Available at: https://azure.microsoft.com/en-us/features/autoscale/
[Accessed 05 04 2020].

Biddix, D. J. P., 2019. *Research Rundowns.* [Online]
Available at: https://researchrundowns.com/quantitative-methods/instrument-validity-reliability/

CAK, 2019. *SECOND QUARTER SECTOR STATISTICS REPORTFOR THE FINANCIAL YEAR 2018/2019,* Nairobi: Communications Authority of Kenya.

CBK, 2016. *Mobile Payments.* [Online]
Available at: https://www.centralbank.go.ke/national-payments-system/mobile-payments/
[Accessed 19 10 2016].

Connect, M., 2018. *Digital & Mobile financial transaction fraud 2018,* s.l.: Myriad Connect.

Cooper, D. & Schindler, P., 2014. *Business Research Methods.* 14th ed. New York, NY: Irwin/ McGraw-Hill.

Corella, F. & Lewison, K., 2012. *Strong and Convenient Multi-Factor Authentication onMobile Devices,* s.l.: researchgate.

Dossey, A., 2019. *Biometric Authentication For Convenience in Mobile Banking: What Banks Need to Know.* [Online]
Available at: https://clearbridgemobile.com/biometric-authentication-for-mobile-banking/
[Accessed May 2020].

DR. Willy, M. & Opili, E., 2015. Factors Influencing the Use of Mobile Banking in Kenya, the Case of M-KESHO in BUNGOMA County. *International Journal of Management and Commerce Innovations ISSN 2348-7585,* pp. 149-1544.

Israel, G. (., 2018. *Determining Sample Size. University of Florida IFAS Extension.,* s.l.: statisticshowto.datasciencecentral.com.

Julian Fietkau, J.-P. S. S., 2020. *Swipe Your Fingerprints! How Biometric Authentication,* s.l.: https://www.usenix.org/.

Luvanda, A., 2014. Proposed Framework for Securing Mobile Banking Applications from Man in the Middle Attacks. *Journal of Information Engineering and Applications,* pp. 20-27.

Oates, B. J., 2006. *Researching Information Systems and Computing.* s.l.:Sage Publications.

Ochieng , O. & Watson , M., 2014. *The Mobile Banking Survey,* Nairobi: Kenya Bankers Association Centre for Research.

Samsung, 2020. [Online]
Available at: https://insights.samsung.com/2020/02/12/which-biometric-authentication-method-is-the-most-secure-2/
[Accessed 14 03 2020].

Santovec, M. L., 2016. Going Mobile? Assessing the Pros/Cons of Mobile Banking. *Wisconsin Community Banking News,* pp. 4-12.

Sarhan, H. H. A. A. &. S. A., 2015. Secure Android-based Mobile Banking Scheme. *118,* pp. 21-26.

Schneier, B., 2019. *Schneier on Security.* [Online]
Available at: https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

Stackify, 2020. *Stackify.* [Online]
Available at: https://stackify.com/soap-vs-rest/
[Accessed 04 02 2020].

Stephen J. Tipton, D. J. W. I. C. S. a. Y. B. C., 2014. Authentication Methods,Permissions, and Potential Pitfalls with Touch ID. *International Journal of Computer and Information Technology,* 03(2279 – 0764), pp. 6-8.

Uppal, D. R., 2014. Transformation in banks in a highly competitive E-Age through E-services -An Empirical study. *Indian journal of Management,* pp. 17-30.

usenix.org, 2020. *BCrypt Algorithm.* [Online]
Available at:
https://www.usenix.org/legacy/events/usenix99/provos/provos_html/node5.html#sec:bcrypt
[Accessed 10 04 2020].

APPENDICES

Work Schedule:

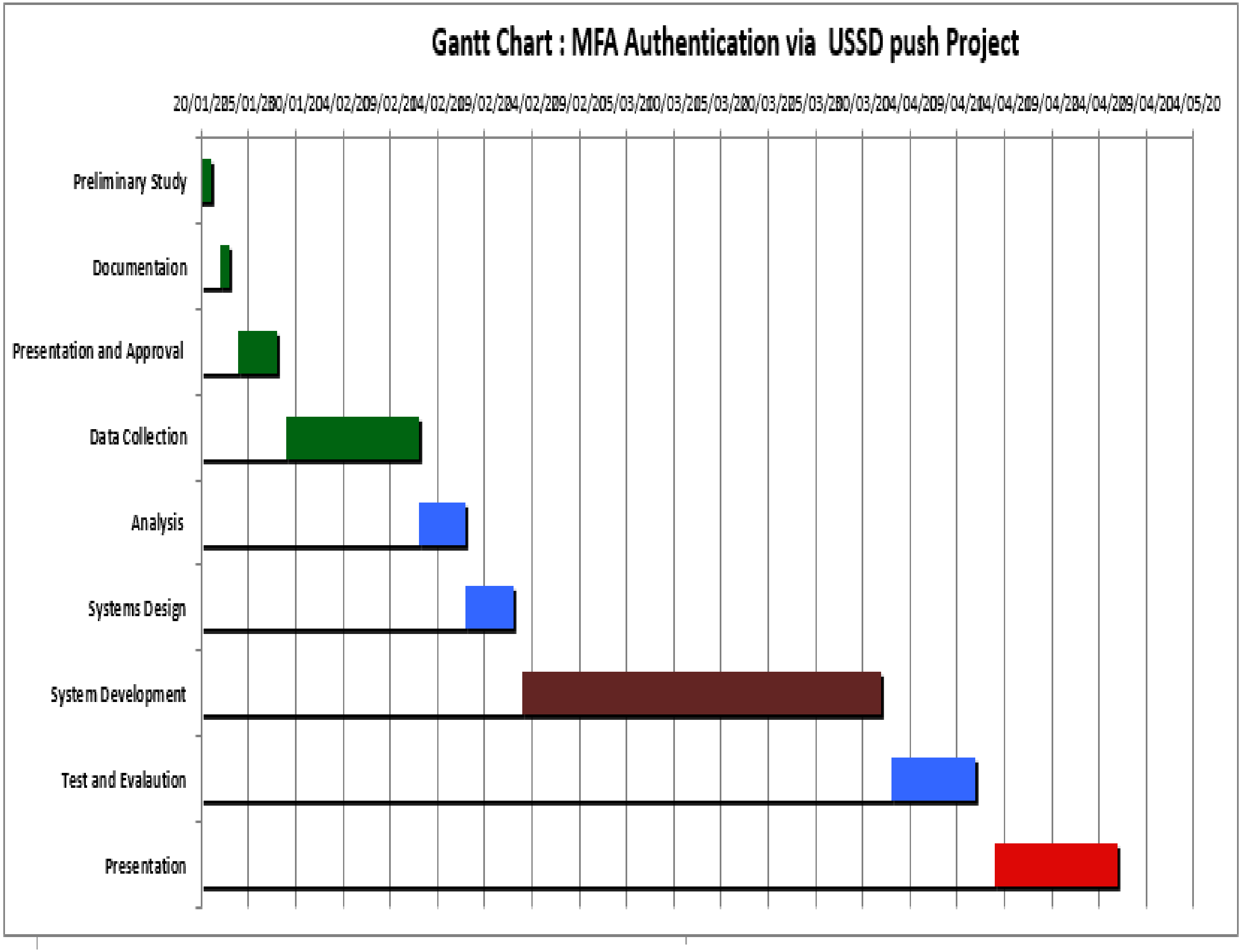
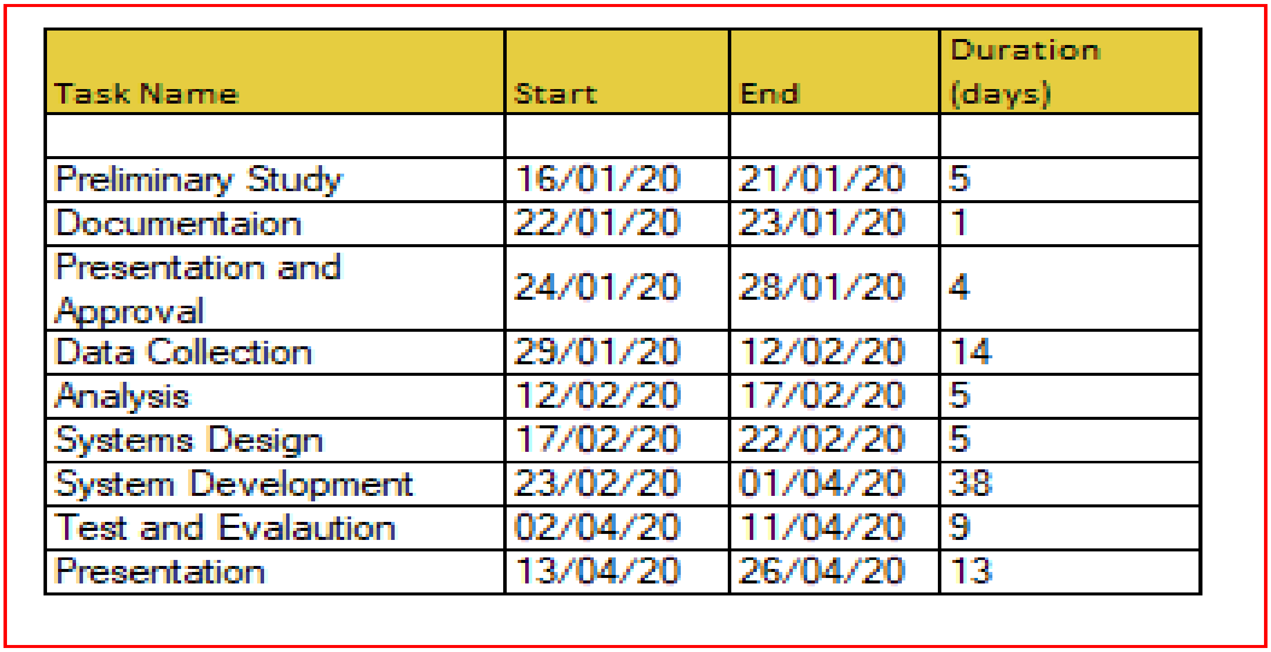


Figure 32: Gantt Chart for the Project

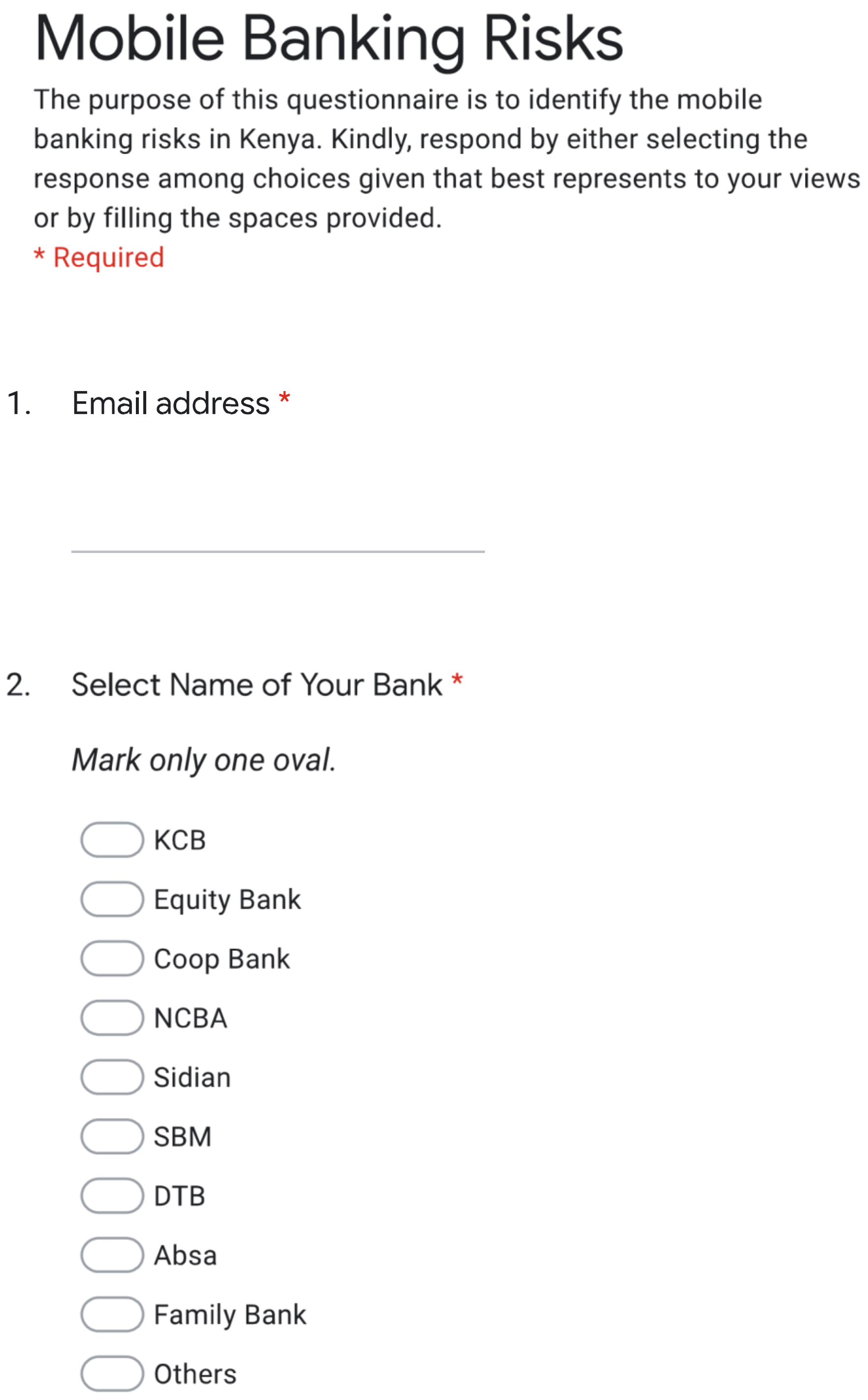


Task Name	Start	End	Duration (days)
Preliminary Study	16/01/20	21/01/20	5
Documentaion	22/01/20	23/01/20	1
Presentation and Approval	24/01/20	28/01/20	4
Data Collection	29/01/20	12/02/20	14
Analysis	12/02/20	17/02/20	5
Systems Design	17/02/20	22/02/20	5
System Development	23/02/20	01/04/20	38
Test and Evalaution	02/04/20	11/04/20	9
Presentation	13/04/20	26/04/20	13

Table 8: Project Activity Schedule

Research Questionnaire

https://docs.google.com/forms/d/1ffXxNS43i6pP8IyRuPBn0Bq_WcBMyr1zQ5-Qx96p0E8/edit?no_redirect#responses



Mobile Banking Risks

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

* Required

1. Email address *

____

2. Select Name of Your Bank *

Mark only one oval.

○ KCB

○ Equity Bank

○ Coop Bank

○ NCBA

○ Sidian

○ SBM

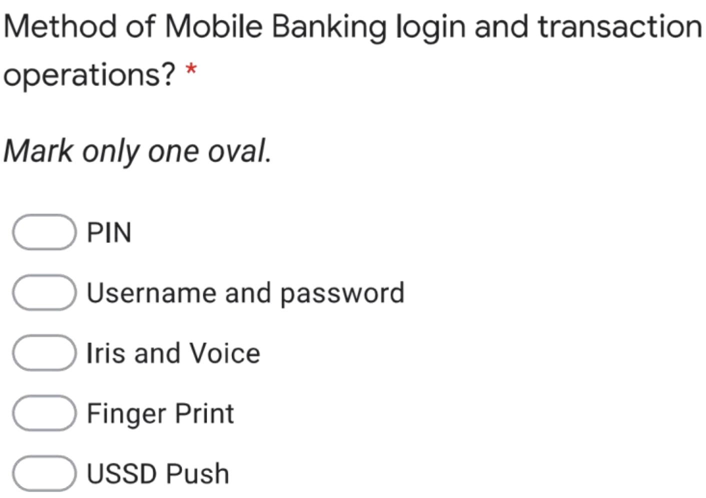
○ DTB

○ Absa

○ Family Bank

○ Others

3



Method of Mobile Banking login and transaction operations? *

Mark only one oval.

○ PIN

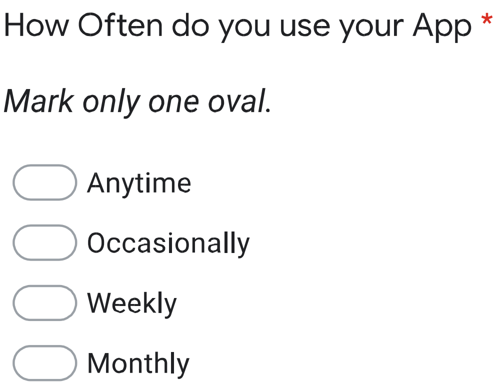
○ Username and password

○ Iris and Voice

○ Finger Print

○ USSD Push

4.



How Often do you use your App *

Mark only one oval.

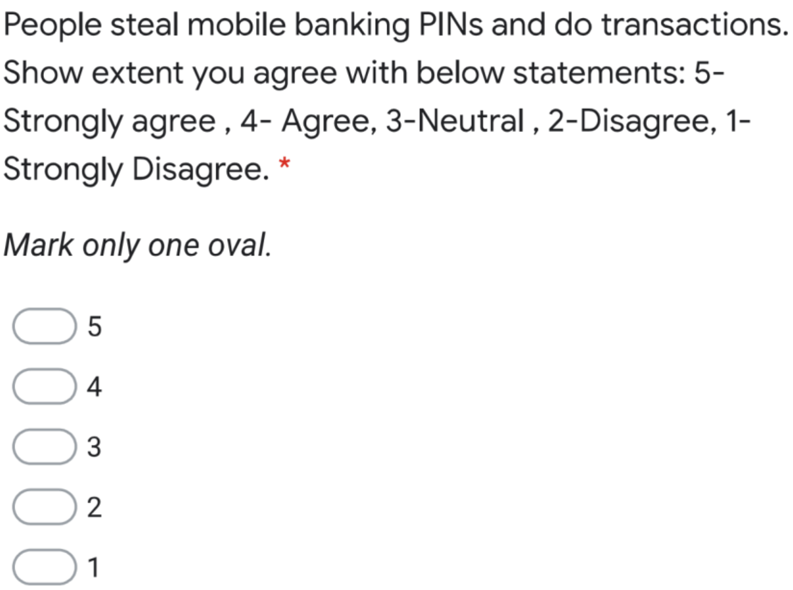
○ Anytime

○ Occasionally

○ Weekly

○ Monthly

5



People steal mobile banking PINs and do transactions. Show extent you agree with below statements: 5-Strongly agree , 4- Agree, 3-Neutral , 2-Disagree, 1-Strongly Disagree. *

Mark only one oval.

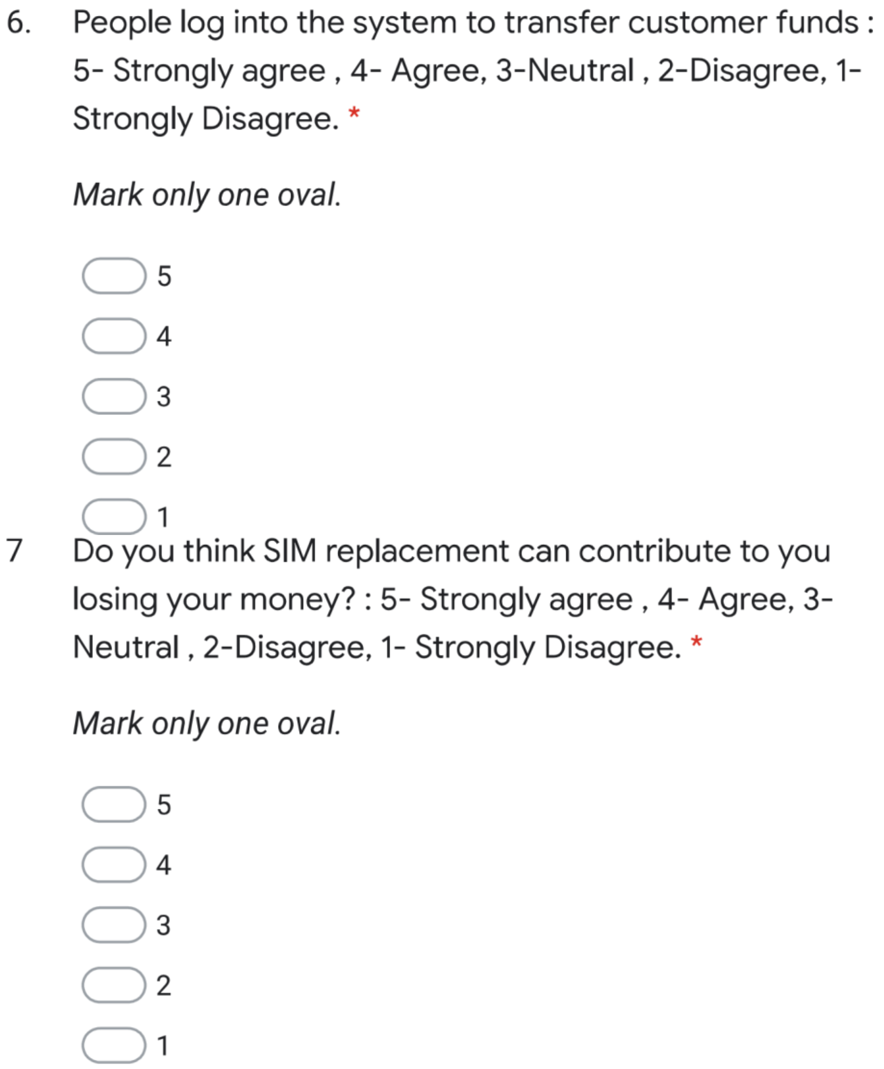
○ 5

○ 4

○ 3

○ 2

○ 1



6. People log into the system to transfer customer funds : 5- Strongly agree , 4- Agree, 3-Neutral , 2-Disagree, 1- Strongly Disagree. *

Mark only one oval.

○ 5

○ 4

○ 3

○ 2

○ 1

7 Do you think SIM replacement can contribute to you losing your money? : 5- Strongly agree , 4- Agree, 3- Neutral , 2-Disagree, 1- Strongly Disagree. *

Mark only one oval.

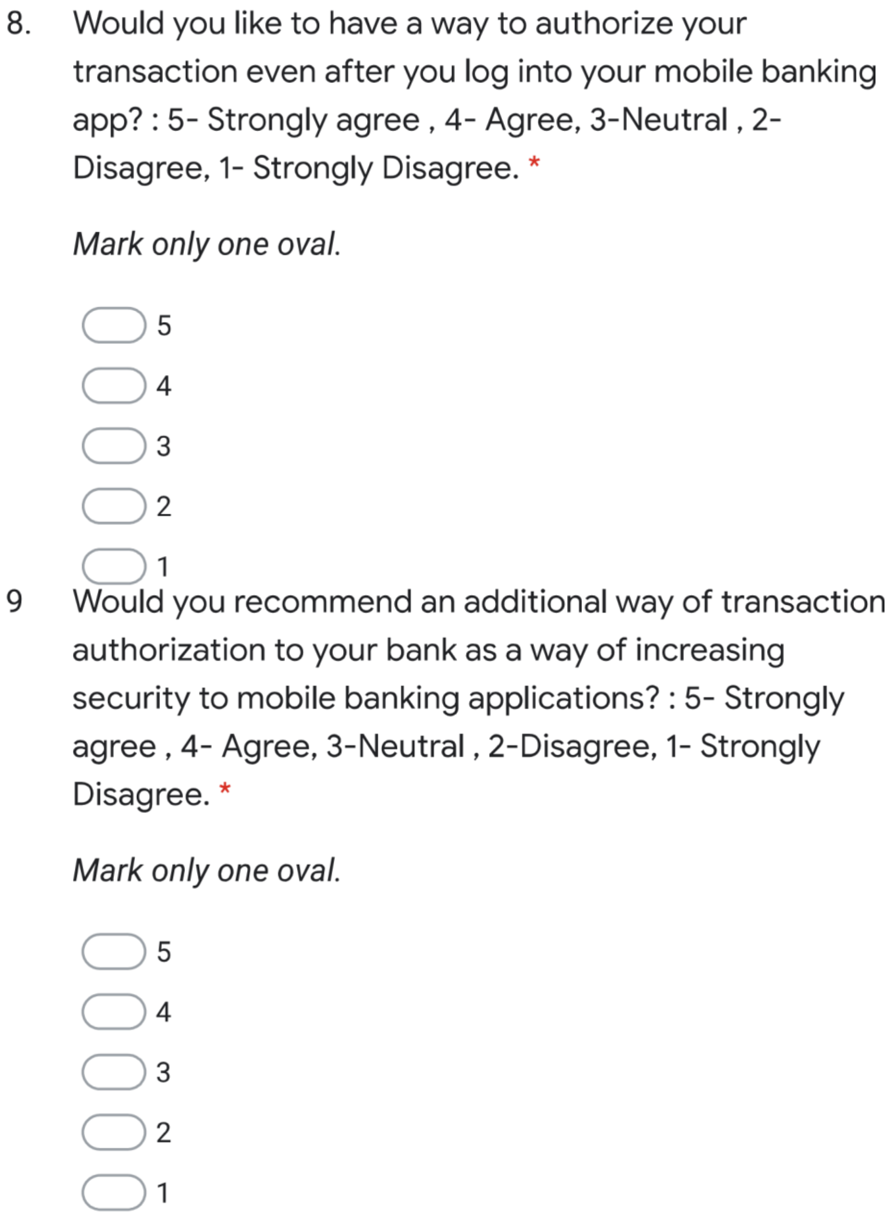
○ 5

○ 4

○ 3

○ 2

○ 1



8. Would you like to have a way to authorize your transaction even after you log into your mobile banking app? : 5- Strongly agree , 4- Agree, 3-Neutral , 2-Disagree, 1- Strongly Disagree. *

Mark only one oval.

○ 5

○ 4

○ 3

○ 2

○ 1

9 Would you recommend an additional way of transaction authorization to your bank as a way of increasing security to mobile banking applications? : 5- Strongly agree , 4- Agree, 3-Neutral , 2-Disagree, 1- Strongly Disagree. *

Mark only one oval.

○ 5

○ 4

○ 3

○ 2

○ 1

10. Do you think using PIN alone to log in and do transactions is insecure? : 5- Strongly agree , 4- Agree, 3-Neutral , 2-Disagree, 1- Strongly Disagree. *

Mark only one oval.

○ 5

○ 4

○ 3

○ 2

○ 1

11. Does your Bank send you a one time pin during mobile transaction? *

Mark only one oval.

○ Yes

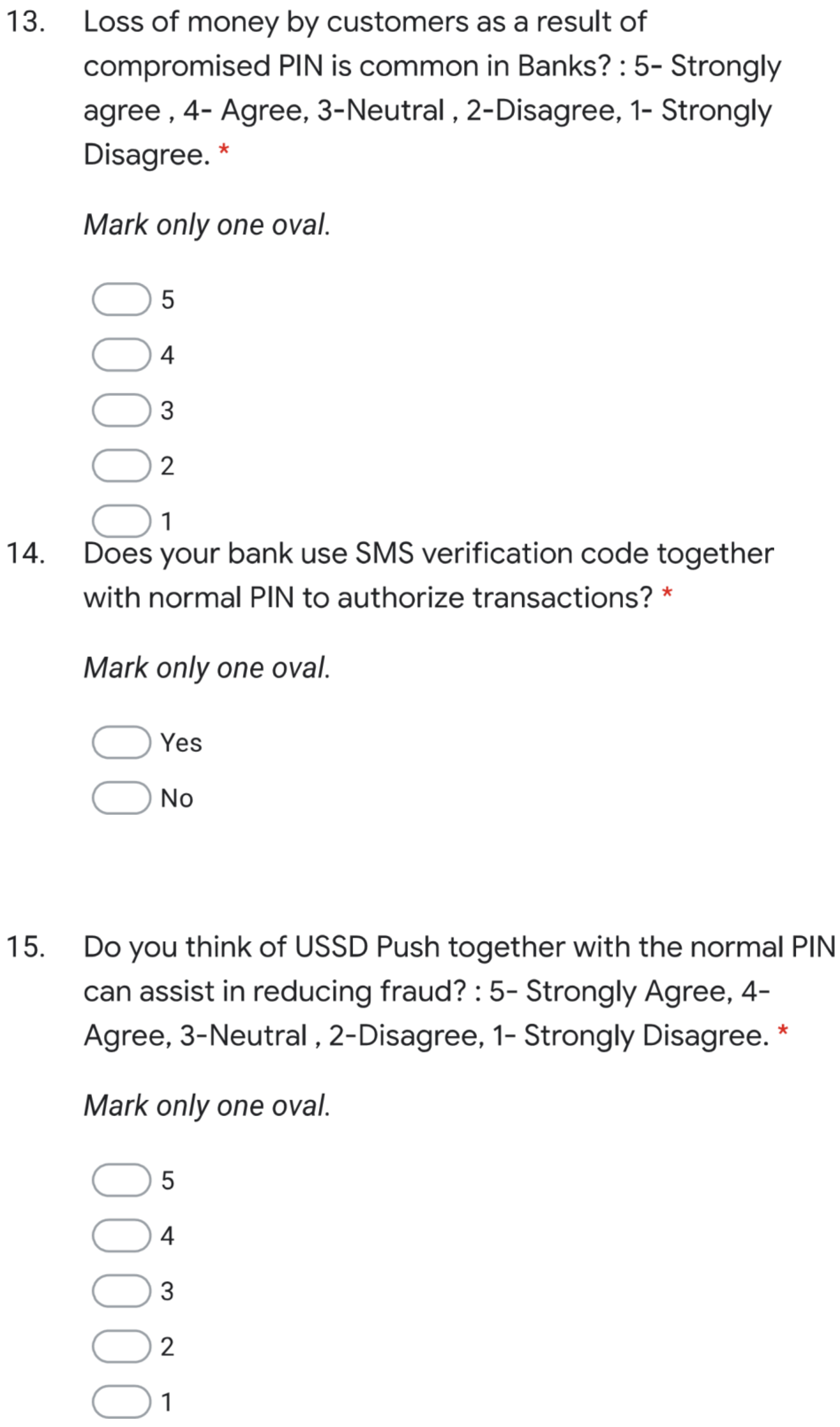
○ No

12. Does your Bank send you a PIN during mobile banking registration? *

Mark only one oval.

○ Yes

○ No



13. Loss of money by customers as a result of compromised PIN is common in Banks? : 5- Strongly agree , 4- Agree, 3-Neutral , 2-Disagree, 1- Strongly Disagree. *

Mark only one oval.

○ 5

○ 4

○ 3

○ 2

○ 1

14. Does your bank use SMS verification code together with normal PIN to authorize transactions? *

Mark only one oval.

○ Yes

○ No

15. Do you think of USSD Push together with the normal PIN can assist in reducing fraud? : 5- Strongly Agree, 4- Agree, 3-Neutral , 2-Disagree, 1- Strongly Disagree. *

Mark only one oval.

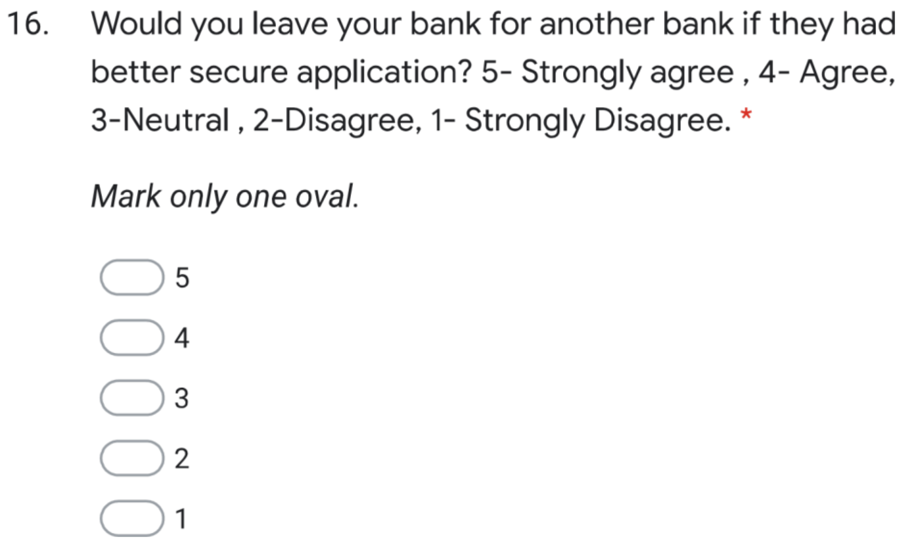
○ 5

○ 4

○ 3

○ 2

○ 1



16. Would you leave your bank for another bank if they had better secure application? 5- Strongly agree , 4- Agree, 3-Neutral , 2-Disagree, 1- Strongly Disagree. *

Mark only one oval.

○ 5

○ 4

○ 3

○ 2

○ 1

Mobile Banking Application Evaluation

The purpose of this questionnaire is to Evaluate the mobile banking android prototype shared via email. Kindly, respond by either selecting the response among choices given that best represents to your views or by filling the spaces provided. Please respond with N/A if you feel you don't want to fill a blank space.

* Required

1. Email address *

____

2. Choose Gender *

Mark only one oval.

○ Male

○ Female

○ Prefer not to say

3. Please select Age bracket *

Mark only one oval.

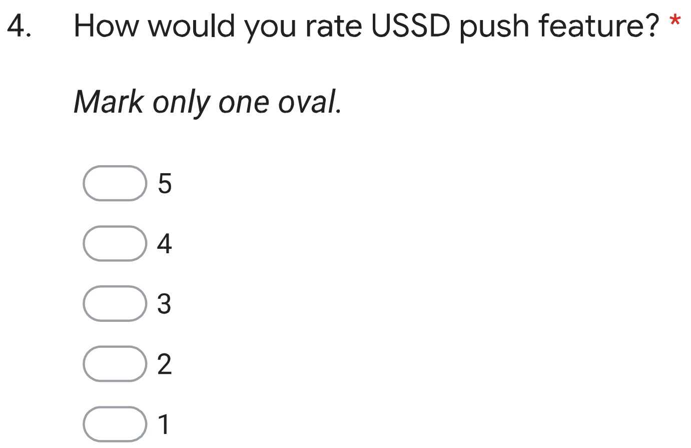
○ 18-24

○ 25-34

○ 35-44

○ 45-54

○ 55-Above



4. How would you rate USSD push feature? *

Mark only one oval.

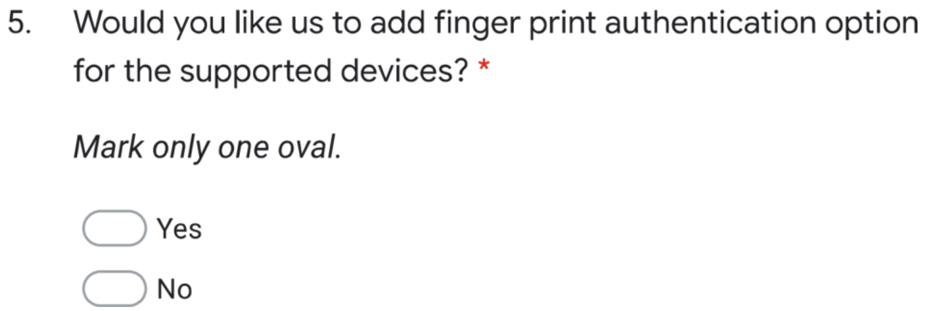
○ 5

○ 4

○ 3

○ 2

○ 1

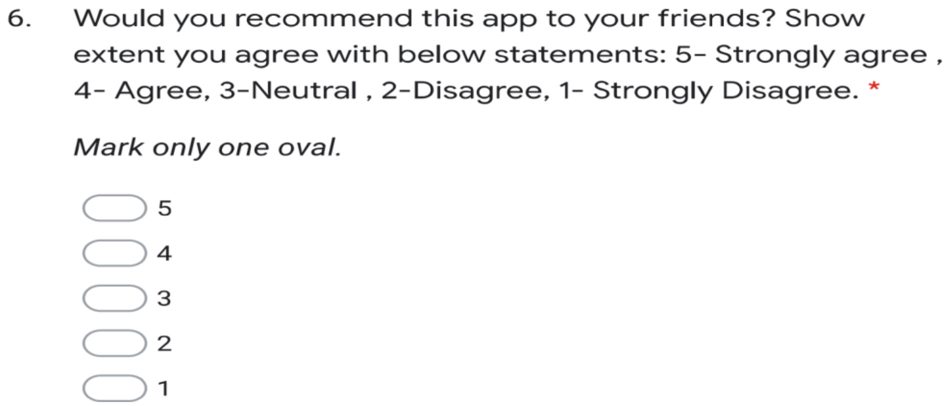


5. Would you like us to add finger print authentication option for the supported devices? *

Mark only one oval.

○ Yes

○ No



6. Would you recommend this app to your friends? Show extent you agree with below statements: 5- Strongly agree , 4- Agree, 3-Neutral , 2-Disagree, 1- Strongly Disagree. *

Mark only one oval.

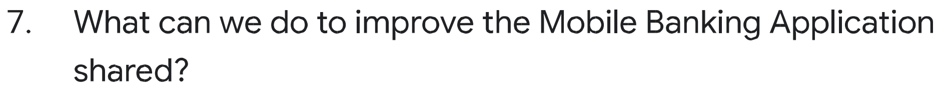
○ 5

○ 4

○ 3

○ 2

○ 1



7. What can we do to improve the Mobile Banking Application shared?