IMPROVED SECURITY MECHANISM FOR MOBILE BANKING TRANSACTIONS: THE CASE OF ETHIOPIAN MOBILE BANKING SYSTEM

A Thesis Presented

By

HENOK BAYU

To

The Faculty of Informatics

Of

St. Mary's University

In Partial Fulfillment of the Requirements

for the Degree of Master of Science

February 2018

ACCEPTANCE

IMPROVED SECURITY MECHANISM FOR MOBILE BANKING TRANSACTIONS: THE CASE OF ETHIOPIAN MOBILE BANKING SYSTEM

By

HENOK BAYU

Accepted by the Faculty of Informatics St. Mary's University, in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Science

Thesis Examination Committee:

Internal Examiner

External Examiner

Dean, Faculty of Informatics

February 2018

DECLARATION

I, the undersigned, declare that this thesis is my original work; all sources of materials used for the thesis have been duly acknowledged. I further confirm that the thesis has not been submitted either in part or in full to any other higher learning institution for the purpose of earning any degree.

Full Name of Student

Signature

Addis Ababa

Ethiopia

This thesis has been submitted for examination with my approval as advisor

---

Full Name of Advisor

Signature

Addis Ababa

Ethiopia

February 2018

Acknowledgments

First of all, thanks to the Almighty God for giving me the wisdom and the strength to start and finalize this study. I would like to thank my advisor Asrat Mulatu for his continuous support of my thesis, for his patience, motivation, enthusiasm, and immense knowledge. He has shown me the right path of research and encouraged me to move forward throughout the study. I would also like to extend my sincere gratitude to Wondante Tolera whose insight, research expertise, and patience provided the basis for my study. He assists me on any challenges of my work.

At last special thanks go to my family. Words can't express how grateful I am to my beloved mother for all of the sacrifices that you have made on my behalf. Your prayer for me was what sustained me this far. They always supporting and encouraging me with their best wishes propelling me towards my goal.

Table of Contents

List of Acronyms

AES	Advanced Encryption Standard
CBE	Commercial Bank of Ethiopia
DES	Data Encryption Standard
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
ISP	Internet Service Provider
MAC	Message Authentication Code
MBS	Mobile Banking Service
MNO	Mobile Network Operator
MSISDN	Mobile Station International Subscriber Directory Number
NBE	National Bank of Ethiopia
PIN	Person Identification Number
RAQ	Random Question
RQA	Random Question Answer
SIM	Subscriber Identifier Module
SMS	Short Message Service
SMSC	Short Message Service Center
STK	Subscriber Identifier Module Toolkit
USB	Universal Serial Bus
USSD	Unstructured Supplementary Service Data
WAP	Wireless Application Protocol
WIG	Wireless Internet Gateway

List of Figures

List of Tables

Abstract

Mobile banking is attractive and convenient approach to perform remote banking services from anywhere and anytime by bank customers. However, there are security deficits in the present mobile banking implementations. Most mobile banking services are established on GSM/SMS. GSM is utilized for data transmission where is sends data in plaintext without any security features. However, financial service providers tend to rely on the security services extensions provided by the GSM infrastructure which has been proved to be susceptible to security attacks related to mobile technologies. The objective of this study is to improve user authentication and end to end security mechanism to enhance the reliability, confidentiality and integrity of SMS based mobile banking services across mobile networks. This work proposes user managed randomly generated question information using pre-saved question and answer on server for authentication mechanism with end-to-end encryption facility to enhance data protection across mobile networks. To do so, assessment on the existing mobile banking service in Ethiopia has been conducted. Based on the assessment on banking reports, related literature and own experience. Finally a prototype is developed for mobile banking services. This work address issues of data confidentiality, user authentication and message integrity in order to provide authentication and end-to-end security for data carried on GSM networks.

Keywords*: mobile banking, GSM security, banking services, user management, pre-saved question and answer, random generation, password*

Chapter One

Introduction

1.1 Background

Recently, mobile services are being adopted increasingly in developing countries because of the availability of mobile device and mobile networks. According to the International Telecommunication Union (ITU) estimation, by the end of the year 2012 there were 6.8 billion global mobile subscriptions and it is predicted by Portion Research in its, "Mobile Fact book 2013" that by the end of 2016 the global subscribers will reach 8.5 billion[1]. In addition, according to the Ethiopian Telecommunication Corporation the total subscription in Ethiopia currently, is more than 52 million as compared to 28 million subscribers in 2009[2]. This shows that mobile technologies are rapidly being adopted both locally and globally and along with it there is a significant growth of mobile services. The increasing number of subscribers is opening up new business ventures and is providing financial institutions additional channels to deliver their services. However, the mobile banking security is still found vulnerable to attacks that will create destruction to the banks and its customers since, it uses simple authentication for identification of customers to perform various financial transactions.

Wikipedia defines mobile banking as the provision and availability of banking and financial services with the help of mobile telecommunication devices [3]. These schemes are highly promoted recently in Ethiopia with varieties of services like withdrawal/balance checking, money transfers, perform payments among others etc. These services are offered in collaboration with telecommunication operator and banking institutions. As a service evolves, new functions and features continue to be added to it. This reduces the time and resources consumed for financial transactions, as one can just use mobile for banking services to make huge transactions worth several millions in just a matter of seconds, without visiting a banking branch. Further, long queues in banking halls either disappear or reduce in most countries.

At the moment, most of the commercial banks provide mobile banking through two channels: through the WAP (Wireless Application Protocol) over GPRS (General Packet Radio Service) and SMS (Short Message Service) using the WIG (Wireless Internet Gateway).

The Global System for Mobile Communications (GSM) began in 1982 for the purpose of investigating and developing a public land mobile system. This was motivated by the rapid growth of analogue cellular systems in Europe around 1980's with each country developing different systems and incompatible with all others in equipment and operation has become a challenge [4]. Mobile banking service (MBS) technologies operated using Unstructured Supplementary Service Data (USSD), Short Message Service (SMS) and Subscriber Identity Module Toolkit (STK) are three popular access technologies used in MBS in the East Africa [5]. USSD is a protocol used in GSM for supporting communication between mobile phones and service provider computers. USSD enables a real-time "session" to be initiated between the mobile user and the USSD application platform. When the service is invoked, it permits data to be sent back and forth between the mobile user and the USSD application platform until the USSD service is completed [6]. Once the session terminates the USSD application platform may be configured to allow SMS to be sent to the user via Short Message Service Center (SMSC) in a GSM network. With STK, the user has an application on the SIM card that is accessed from the phone's menu [7].However; security concerns are on the rise in all areas by financial institutions and their customers (users) to make mobile banking services reliable in the day to day financial transactions. Hence, government organizations are setting security standards, passing laws and forcing organizations and agencies to comply with these standards with non-compliance being met with wide-ranging consequences. For example, according to[8], National Bank of Ethiopia (NBE) orders all financial organizations to integrate their service with information security framework.

The current security models in use on mobile banking systems are based on several security layers, with many security mechanisms and solutions, all aimed at providing good security for mobile banking systems, applications and transaction data, providing identification, authentication and authorization. But, there are several threats and attacks in mobile communication that are ever-evolving, and financial institutions and users are cautious of the risks.

Among today's growing concerns are:

- Mobile Malware - Trojans, viruses and root kits migrating from traditional online banking and designed specifically for the mobile service.
- Third-Party Apps - Consumers are being friendship with their mobile applications, but often these apps come from third parties with questionable security practices.
- Unsecured Wi-Fi - is a toll-free highway for fraudsters to gain access to mobile devices, either to seize control of or gain access to account information.
- User Behavior - are prone to download third-party apps to use unsecured wireless networks to open and click links in SMS text messages and e-mails, and lose their mobile device [4].

This study mainly focuses on the assessment of the challenges of mobile banking security threats and attacks in the GSM network. The goal is to build a reliable mechanism for authentication and end to end security for portable devices that ensure users to securely perform banking services via SMS using GSM network.

1.2 Statement of the Problem

Ethiopian banks, such as Commercial Bank of Ethiopia and others have introduced the Wireless Internet Gateway (WIG) for mobile banking. They use the Unstructured Supplementary Services Data (USSD) with SMS approach. The banks require the user to first send a USSD string with the user's PIN to the banking server. Then the server returns a message to notify the user that the server is ready to accept banking SMS message. This approach is not secured because user's detail is transmitted in plaintext.

The mobile network operator has full access into the banking details sent by the user. In addition, the initial idea for SMS usage was intended for subscribers to send non-sensitive messages across the open GSM network mutual authentication, text encryption, end-to-end security, and non-repudiation were omitted during the design of the original GSM architecture [5].

Even though most of the banks in Ethiopia have taken mobile banking as one of their core services to their customers, it can possibly suffer from various security breaches discussed in [5]. Therefore, NBE announce to all financial organizations to integrate security framework for their information system. This framework will include technical, physical and administrative components.

In the technical component, mobile banking security solutions can be considered as one of the vital elements to protect users' information and operations from security shortfalls [8].This development process costs around 80 million dollar and has to be completed within 2-5 years. Personal work experience on mobile banking indicates that user's acceptance of using these services is much below average. The current authentication mechanism for the service is only PIN (personal identification number) which is not enough to authenticate users. It may be vulnerable for eavesdroppers [5]. Ethiopian banks have questions on the security of customer's confidential information which is apparently the biggest issue raised by banker. Thus these scenarios motivated this work.

Currently there are many researches of mobile banking security conducted to enhance its security. T. Takada and H. Koike in [16] proposed to use image as password instead of text passwords for authentication enhancement. Chikomo et al in [6] designed a mobile payment system integrated with biometric authentication model that provides the facility of mobile payments with increased security levels. Nikhil and Mithil in [21] proposed a framework for providing end-to-end security for transmission of SMS. In this framework they used A8 encryption algorithm for maintaining confidentiality. M.hassinen in [28] has used RSA algorithm in his work to encrypt SMS messages used in mobile commerce, whereas keys are generated using SHA-1. Despite these studies will not consider the users who don't use smart mobile phone and apply an algorithm which is proved that not enough secure. Even if successful security enhancement implementation is achieved; it is not a sufficient condition to fully benefit all banking users. Rather, it also demands continued efforts on better end to end security algorithm, user friendly and authentication must consider all types of mobile phones. There is a need for a better implementation of security mechanisms for SMS-based mobile banking operations by identifying attacks and treat with possible solution to ensure a secured transaction. So, the main study question is to answer, how to build a generic effective user authentication mechanism in SMS-based mobile banking system adding user-managed information?

Hence, this study explores and gives solution for

- User authentication
- Client and server communication security

1.3 Objectives

1.3.1General Objective

The major objective of this study is to design an improved mobile banking user authentication mechanism and user-to-server security mechanism to enhance the reliability, confidentiality and integrity of SMS based mobile banking services across mobile networks.

1.3.2 Specific Objectives

- Understand the existing principles and practices on mobile security mechanism and measure using gaps analysis especially for SMS based communication across GSM networks.
- Identify the requirements to secure mobile banking user authentication mechanisms/approaches.
- Propose a reliable mobile banking user authentication and a secure communication mechanism between the mobile and the server that ensures better financial transactions.
- Design a prototype for securing mobile banking user authentication and user-to-sever security mechanisms using open source tools and technologies.
- Test the proposed solution in mobile banking operation scenarios.

1.4 methodology

This study has attempted to design an improved user authentication and user-server security mechanism in Ethiopian mobile banking transaction. This chapter presents the methodology that is used to achieve the objective of the study. In order to achieve the research objectives mentioned above, design science approach is applied. The customized methodology employed in this work mainly consists of four activities as stated below:

Step I: Understanding users (questionnaire and interview survey)to identify the requirements of the existing mobile transaction

Unlike designing a product for a specific group of people, here this work designs for a broad range of people. Therefore there need a method that allows to discover a variety of subjects. In this work interviewees and list of preset questions followed by a discussion with some open-ended questions are used.

The sample of the interviewed subjects was small, the data collected from the interviews provided that sufficient understand of people‘s habits of using mobile phones and their perception of the security of mobile phones.

From the interview of this work discovers the following list summarizes the reason that learned from interviewees

- Prefer to go to the bank to do banking with face-to-face interaction.
- Preference of cash transactions over digital transactions.
- A mobile phone does not give enough details
- A third party might have access into the account information.
- Easy to share pass codes for others.
- Works only with one language

Step II: Conduct literature review to identify the requirements of the existing mobile transaction

A thorough literature review has been conducted to determine the extent of knowledge available in the field of mobile security, in general, and to revisit the principles of authentication of existing security solutions, in particular. The outcome of this activity was a series of treats and attacks which need to be addressed while deploying mobile security-enabled services alongside the existing system.

Step III: Design architecture based on the requirements of the system.

This stage involves developing requirements based on the challenges identified in Step I, and II followed by designing the first prototype for mobile transaction with improved security features. The design has been incrementally enhanced to provide improved security functions such as to secure the banking services. The constituents for prototyping the mobile banking security was also set up during this stage using available methods and tools identified in the literature review.

Step IV: Develop a prototype of the proposed system.

The initial prototype is built to test and evaluate if the designed mobile banking improvement could be established. Once successful, the prototype has been incrementally updated and finally evolved into a more advanced system through a testing and feedback integration cycle.

Step V: Test and evaluate.

Each design and development iteration resulted in the inclusion of new functionalities that are tested and evaluated by using mobile banking service scenarios. Thus, preliminary testing and evaluation has been performed to test the functionality of the designed security mechanisms not only to guarantee their proper working but also to make the fulfill the initial user demand.

1.5 Scope and limitation

This work aimed to develop improved security mechanisms for mobile banking specifically for SMS-based services. It also targeted to improve the existing end to end security mechanisms on mobile banking architecture that are based on data transmission over GSM network environment. It doesn't include, Internet banking services. It focuses only on securing the existing mobile banking services through the newly developed security mechanisms and supports them through the available end to end security algorithms to insure confidentiality, integrity and availability of mobile banking environment.

1.6 Organization of the Rest of the Thesis

The rest of the thesis is organized as follows .Chapter two presents the issues related to mobile banking and GSM network security and reviews related works that have been conducted on mobile banking security. Chapter three will be about the findings on the existing mobile banking system and discuss the proposed solutions. Chapter four will present the prototype implementation of the proposed system .Chapter five presents the evaluation of the improved mobile banking system and finally Chapter six presents the conclusions and future works.

Chapter Two

Review of Literature and Related Works

2.1 Overview

The objective of this chapter is to give description of the research area on mobile banking security with its security concerns, concepts, technologies and efforts show the existing mobile banking service security solutions in mobile banking business models, security concerns, usability, and related issues. This section also tries to analyze existing research and to clearly show the research gap to justify the significance of this study.

The advent of ICT has revolutionized the way the financial services industry conducts business, empowering organizations with new business models and new ways to offer 24/7 accessibility of their service to their customers. The ability to offer financial transactions online has also created new players in the financial services industry, such as online banks, online brokers and wealth managers who offer personalized services, although such players still account for a tiny percentage of the industry [4].

The history of modern banking in Ethiopia goes back to 1900 when an agreement was reached in 1905 between Emperor Minilik II and Mr.Gillivray, the representative of the British owned National Bank of Egypt. As per the National Bank of Ethiopia statistic there were 18 private and 3 state owned banks in 2008. Out of these 19 banks, the state owned Commercial Bank of Ethiopia is the largest and leading bank in financial operations.

Commercial Banks as such provide all the banking services including ATM facility, Internet Banking, Telephone Banking, SMS banking and Mobile Banking beside the traditional banking activities.

The appearance of E-banking in Ethiopia goes back to the late 2001, when the largest state owned, Commercial Bank of Ethiopia (CBE) introduced ATM to deliver the service to the local users. Electronic banking facilities provided by most Ethiopian Banks are very basic.

The rapidly growing information and communication technology (ICT) is knocking the front door of every organization in the world, where Ethiopian banks could never be exceptional. In the face of rapid expansion of electronic payment (E-payment) systems throughout the developed and the developing world, Ethiopian's financial sector cannot remain an exception in expanding the use of the system. At the end 2013/14 fiscal year, there were eighteen commercial banks operating in Ethiopia, of these sixteen are private commercial banks while the rest two are state owned banks. Despite a rapid increase in the number of financial institutions since financial liberalization around 1980's, the Ethiopian banking system is still underdeveloped compared to the rest of the world [9].

The Ethiopian banking industry as a whole had a network of 2,323 branches as of September 30, 2014, in which the average number of population being served by a single branch was around 37,861.8. With urban skewed branch networks it is hard to ensure efficient flow of financial resources and optimize the contributions of the entire financial system to the development processes. The mobile banking development in Ethiopia is at its starting stage.

The idea of using mobile phones for banking has been in practice for almost a decade in the developed parts of the world [10]. Mobile phones are used in the developed world to make banking convenient for people who already hold bank accounts. Mobile banking has now become a significant conduit for monetary flows in the countries where it operate.

2.2 USSD Operation Overview

In USSD, GSM communication technology is used to send messages between a mobile phone and an application server in the network. It is very much similar to SMS, but USSD is session oriented as well as interactive. It does not have store and forward concept. USSD is a session based protocol unlike SMS or MMS; therefore the session needs to be allocated to each and every interaction. Comparing with SMS, the USSD has a much faster response and real-time feature. Due to its capability of interactive dialog, not only USSD is superior to SMS in extending mobile services, but the service carrier can also tailor the USSD services to satisfy local user requirements, with little modification to the original configuration parameters. Figure 2.1 helps to understand the USSD call flows that any request towards USSD, its response and the series of requests and responses for that particular session has the same session ID until it is closed or timed out.

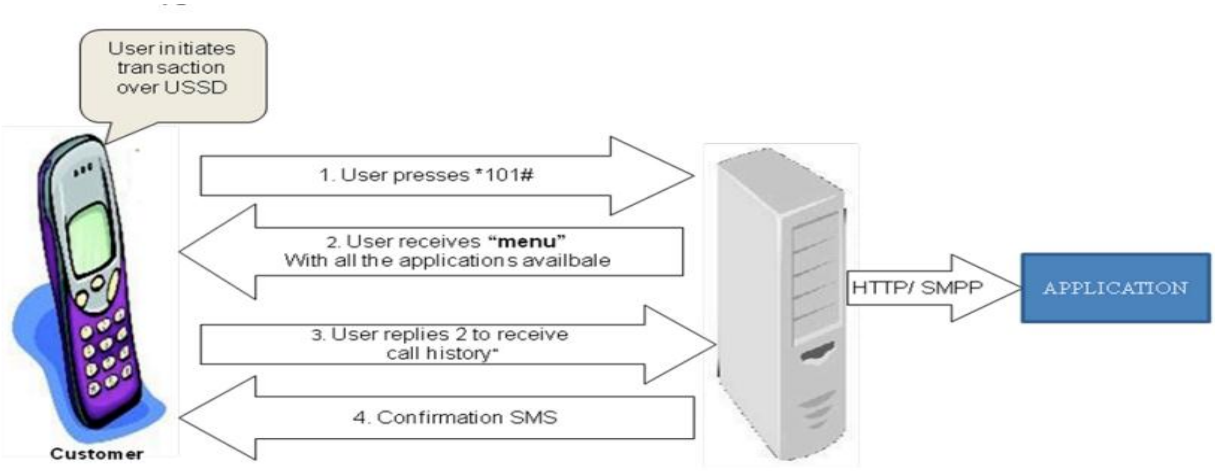


Figure 2.1: USSD call flow adopted from [5]

2.3 Challenges in Mobile Banking Services

As J. Strasburg in [11] stated the main risks that financial institutions face are:

• **Loss of Consumer Confidence**: E-Commerce sites represent a multi-million dollar investment as well as a key revenue generating infrastructure for many businesses, especially those in the financial, retail, online auction and Internet Service Provider (ISP) markets. Every time an institution becomes the victim of an attack, customers lose confidence in the institution's ability to protect them. Consumers feel very vulnerable when they receive phishing emails or hear of new breaches. Any institution, whether it is a government agency, a retailer, or a financial institution suffers a loss of integrity when it becomes a victim of an attack; consumers wonder if the institution can truly protect their identity, when the institution cannot protect itself. Loss of consumer confidence has resulting impacts on the intuitions.

I. Reputation Impact: Once an institution becomes a victim to an attack its image is damaged, it begins to lose face among competitors, and its integrity is questioned by both consumers and competitors.

II. Financial Impact: Some of the costs that are absorbed by a financial institution during and after an attack include response, identification, and clean up. These negatively impacts the normal transaction of the organization

III. Stronger Authentication: Financial institutions must do more to protect themselves and customers from different attacks and data breaches must ensure that consumers feel safe when using mobile banking features.

As stated in [12] an enhanced authentication of the customer at login or while the user is transacting in their account can be implemented in a variety of different ways, many of which are based on the factors of authentication.

- **Multi-Factor Authentication**

Authentication techniques can be split into three categories [13].

I. Something a person knows: password, PIN, mother's name maiden's name.
II. Something a person has: ID card, key fob, or credit card.
III. Something a person is: biometric, voice recognition, fingerprint, facial recognition.

Multi-Factor authentication uses more than one of these factors to make authentication stronger. The more levels used in an authentication system the stronger the authentication. As more factors of authentication are added, the security becomes more reliable and the level of fraud deterrence increases.

I. Something a Person Knows

While something a person knows is the most widely used (including user name and password, or shared secrets), some would argue that it is the least secure form of authentication as it can be easily compromised. The most common example of a shared secret is a password or PIN [14]. However, shared secrets also include questions that require specific knowledge of something about the customer. These are questions such as "Which address have you previously been associated with?" or "What is the name of the city you were born in?" Shared secrets are often selected during the initial enrollment process or can be added as an additional security.

Processes during or after enrollments oftentimes allow customers to select from a list of questions provided by the authenticator or create their own question; then the customer provides the answer to the question. The shared secret then can be used as an additional authenticator when a customer is attempting access. The important thing to remember about shared secrets is that they should be something that is not normally used for authentication purposes and that only the customer would know.

Shared secrets have a low cost to the financial institution, since they can be simply added to the login page and only require the capture of a small amount of additional information [14]. Shared secrets are also very easy to use from a customer stand point. They can be added to a standard login with minimal impact to the customer's login process [14]. They also require no additional hardware for the customer to buy or install.

II. **Something a Person Has**

Something a person has is the second level of authentication; this level represents some sort of physical device that a person has that may be used in a multi factor authentication protocol. This level of authentication is usually considered stronger than "Something a person knows." This authentication level could include tokens such as a USB device, a grid card, a smart card, or a password generator. This level could also include out of band authentication, such as a onetime password that is emailed or provided via text messaging, as well as PC fingerprinting.

III. **Something person is**

Since people forget things and lose things, one might contemplate basing an authentication scheme for humans on something that a person is. After all, we recognize people we interact with not because of some password protocol but because of how they look or how they sound "something they are". Authentication based on "something you are" will employ behavioral and physiological characteristics of the principal. These characteristics must be easily measured accurately and preferably are things that are difficult to spoof. For example, we might use Retinal scan, Finger print reader, Handprint reader, Voice etc.

2.4 SMS Banking

SMS (Short Messaging Service) allows users to send and receive text messages on a mobile phone using the numbered keypad on the handset to input characters. Each message can be up to 160 characters long and sent to and from users of different operator networks. All mobile phones available today support SMS. Indeed, SMS has become a global phenomenon, with billions of text messages sent worldwide every week. In addition to the person-to-person SMS, a large variety of content-based text messaging services are available. The majority of GSM operators offer users the ability to subscribe to services that send news, sport and entertainment content direct to a mobile phone in the form of an SMS.

SMS Banking requires a registered customer to initiate a transaction by sending a structured SMS (SSMS) message to the Mobile Banking Service. This SSMS requires a tag word identifier to instruct the SMS gateway to submit the message to the correct SMS application. A tag word is the first word in the SSMS. The balance of the SSMS would hold the instruction from the customer to the Mobile Banking application. E.g. PIN for SMS banking.

The SSMS would pass from the consumer's handset through the GSM network to the MNO (Mobile Network Operator) SMSC (Short Message Service Centre). A SMSC stores and forwards the SSMS to the SMS Gateway allocated to the short code used by the Mobile Banking Service Provider. The Mobile Banking Service Provider would use the consumer's mobile number, forwarded by the SMSC with the SSMS, to identify the consumer and respond to the consumer's request. The response would follow the same return path and, would respond to the consumer with an SMS confirmation message. E.g. Bank Balance is 150.00.

2.5 Unstructured Supplementary Service Data (USSD)

In its simplest definition, USSD is a menu driven form of SMS where a customer would receive a text menu on its phone as opposed to a string of words. USSD is a data bearer channel in the GSM network. Like SMS, it transports small messages of up to 160 characters between the mobile handset and the network. Unlike SMS, which is 'store and forward', USSD is session based and can provide an interactive dialog between the user and a certain set of applications. In other words, both sides of the dialogue happen during a session whereas an SMS based interaction is broken into each segment of communication between the client and the service.

A registered consumer would dial a number that includes * and #. This number could be saved in the consumer's phone book as the bank's name to avoid confusion in dialing or having to remember the USSD string. An example of a USSD string would be *889#. Once the consumer has entered, and dialed the USSD string, the consumer's request for the service would be passed through the network to the USSD gateway at the MNO, which in turn would recognize who the service provider/bank was and forward the request to that service provider. The service provider would respond by forwarding to the consumer, through the MNO, a text based menu. The consumer would receive this menu on its screen, press the reply button on the phone and enter the number of the option that is required. Example: Press reply, enter 1. To which the service provider would collect the balance information for the consumer and send back a message that says: The Balance of your account is 1000.00.

2.6 Authentication and risk mitigation in mobile banking

PIN authentication is used in almost every implementation, creating a form of digital signature that says the consumer is initiating the transaction from its SIM card and enters secret PIN to prove who the owner of that SIM card is. This is a powerful tool that the mobile operator provides for consumer authentication. Work does need to be done in controlling access to the linking and de-linking of MSISDN(Mobile Station International Subscriber Directory Number)from the SIM card as in some cases this is left to the control of the MNO's distribution channel.

The PIN should be customer selected, and never stored on the mobile banking platform or application as a PIN but rather as a PIN Offset. As an additional measure it is recommended that the customer be asked for certain elements of their PIN for validation (challenge response) as opposed to the full PIN. Dual bearer channel in a single transaction is advised to prevent any possible spoofing or other attacks that will result luck of consumer confidence.

2.7 Current SMS Banking Services in Ethiopia

Currently Ethiopian banks, such as CBE use the USSD with SMS approach that requires users to first send a USSD string with the user's PIN to the banking server then the server returns a message to notify the user that the server is ready to accept banking SMS message. This approach is not secure because every user's detail is transmitted in plaintext. The mobile network operator has full access into the banking details sent by the user. And also the user is open for different security breaches. The SMS approach only requires users PIN for authentication. It's not enough to authenticate the genuine user. The user PIN is too short and easy to grab by intruders. In my own work experience it is reported that there are an average two complains per week related to PIN mishandling.

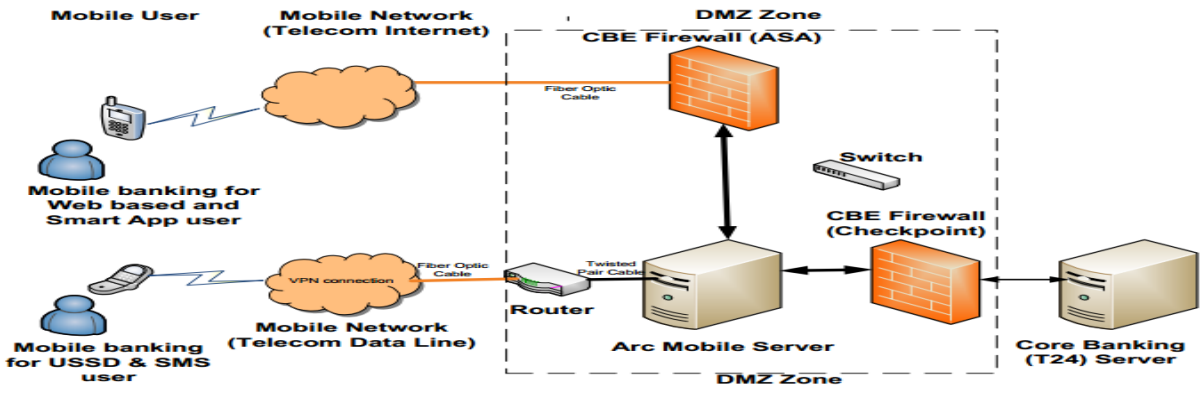


Figure 2.2: Current Architecture of Ethiopian Mobile Banking System

2.8 Security Problems with SMS

The initial idea for SMS usage was intended for the subscribers to send non-sensitive messages across the open GSM network mutual authentication; text encryption, end-to-end security, and non-repudiation were omitted during the design of GSM architecture [11].

I. SMS Encryption

The default data format for SMS messages is plaintext. The only encryption involved during transmission is the encryption between the base transceiver station and the mobile station. End-to-end encryption is currently not available.

II. Authentication

Current authentication mechanism in mobile banking is one factor authentication mechanism the user only authenticated by PIN only. There have to be additional mechanisms to enhance authentication.

According to [10], in order to keep a mobile banking system secure there are seven security requirements that any security service should be able to accomplish:

- Confidentiality: The confidentiality of sensitive information needs to be protected, i.e. unauthorized people should not be able to gain access to personal information.
- Integrity: Mobile service providers need to protect the integrity of data transmitted over wireless networks from the point of transmission to the point of delivery. The system should be able check that the data is the same at the points of origin and destination.
- Availability: This is about ensuring that services are available on demand, which often means 24 hours a day, seven days a week. This is related to security because a security breach can lead to downtime, for example Denial of Service and virus attacks.
- Non-repudiation: Non-repudiation ensures transactions are legally binding. This is critical for electronic banking systems because it prevents complication from regulation violation.
- Authorization: Authorization ensures transactions are endorsed and authorized by the parties involved.
- Authentication: Authentication is the process of identifying the user to be whom they claim to be.

- Privacy: Privacy is a prominent issue in mobile banking. Mobile banking service provider must meet the legal requirements.

With the above security requirements, authentication is a basic building block of security. Once the authenticated communication channels are established, other security services such as confidentiality, privacy, authorization, integrity and non-repudiation can be realized [11].

This work solves the issues of authentication and confidentiality by implementing multi factor authentication on something person knows and AES encryption algorithm without affecting the current system.

In all mobile banking systems the communication between the user phones and the bank server is implemented using GSM-based services like SMS or USSD and acknowledgements from the bank server are also sent using the same channels. In order to protect the system from forgery, banks must implement methods to ensure that the sender of every transaction request SMS or USSD message can be accurately verified. Different mobile banking systems use different authentication techniques depending upon the amount of control they have on the network protocols. Current Ethiopian mobile banking system uses a PIN-based approach to authenticate users to the bank: messages are sent using USSD and since the provider of the service has complete control of the network, a proprietary encryption program is installed on users' SIM cards to protect the PIN during transmission. Details of the encryption are not publicly known. PINs are used, too, but they are transmitted in plaintext as part of SMS-based transaction messages. Such a solution does not guarantee good security since GSM's inbuilt encryption algorithms have several reported weaknesses is described in[15] which may cause PINs to be compromised.

Many countries with mobile communication services use Global System for Mobile Communication (GSM) architecture to network their mobile connections. GSM network was initially designed to be used for voice communication. As the usage of mobile phone increases, people begin to use their mobile phones for additional means of data transmissions.

The most popular type of data transmission is Short Message Service (SMS). This service allows the user to send plaintext messages to the destination mobile phones. The advantages of using SMS are that it is relatively inexpensive and it is reliable for sending non-sensitive messages. SMS messages are sent asynchronously.

When a message is submitted for sending, the service provider will keep the sending message in its message buffer until the message is delivered to the destination mobile phone.

Mobile banking is a convenient method to let those who struggle to access bank services to have an easier banking approach. The intention of mobile banking is to reach out to the unbanked population and to provide them a low cost banking scheme.

Banks offer mobile banking services which allow their customers to transmit their banking details via SMS messages. SMS banking service is convenient in terms of the user can perform mobile banking in anytime and anywhere fashion. The transmission speed of SMS messages is generally fast and delivery is reliable.

The user can expect their transactions to be transmitted and performs in real time. The problems with SMS banking are that the SMS message is not entirely secured. There are many flaws in the GSM architecture which lead to security shortfalls for SMS banking.

According to research publications related to security in mobile banking services and GSM are reviewed and analyzed [4] [10]. The focus is on issues related to provision of end-to-end security, mutual authentication, message integrity and effective server security management policies. Hash functions, message authentication codes and digital signatures mechanisms in securing financial transactions over distrusted networks have been done in [10].Depending on the nature of the organization providing the scheme Dermish et al.[4] distinguished between bank-based and non-bank-based mobile banking models.

In some researches carried out on mobile banking adoption, emphasis is given for the impact of social and cultural factors such as perceived credibility, facilitating conditions, perceived elicitation and demographic factors to adopt mobile banking by consumers [7]. In addition, consumers may hesitate to use mobile banking services for security reasons. The security concern emanates from the nature of mobility and the inherent weakness of wireless infrastructure.

T. Takada and H. Koike in [16] proposed to use image as password instead of text passwords. Although mobile phone penetration is better than the conventional banking service to reach the unbanked in developing countries, there is a challenge of using mobile banking applications easily by the poor peoples who don’t have smart phone [17].

According to Medhi in [17], non-text designs like spoken dialog and rich multimedia are strongly preferred over text-based for such users. Several studies have shown a great concern of security issues in mobile money services as of Emmanuel, A. and B. Jacobs in [5] highlighted several fraud cases that threaten the security of mobile money services (MMSs) including false transactions, misuse of PINs and identity theft. The study found that MMS operators are aware of the need to improve mobile money security and that improved security in MMSs will enable operators to protect themselves, their customers and agents, and assists successful provision of mobile money business.

Many scholars [8][11] argued that mobile money users who need assistance in processing transactions are more probable to share their PINs compared to users who do not need assistance. Works on security and privacy concerns of mobile money users in Africa revealed that if proper measures to secure mobile phones are not taken, mobile phone users might be vulnerable to criminal attacks [11].

There have been some proposals to use voice biometrics for authenticating users in mobile banking [18]. However, to the best of our knowledge, none have been deployed at scale, even though voice-based authentication systems have been shown to work in the laboratory [18], the problem of ambient noise in developing world environments makes them extremely difficult to deploy in mobile banking. Currently some companies in India use fingerprint biometrics to authenticate users in agent-assisted banking but the setup and operational costs of these solutions are significantly greater than that of token-based systems.

Biometric authentication mechanisms are preferable methods for providing the highest security to the mobile payment in e-banking, [16]. In different proposed models, fingerprint image is taken in real time and sent to the server for authorization. A fuzzy logic based fingerprint matching algorithms are used in the server side for authorization.

Chikomo et al., in [6] designed a mobile payment system integrated with biometric authentication model that provides the facility of mobile payments with increased security levels. The problem is that the user must have smart phones to use this kind of authentication mechanism. This work will help users to use mobile payment system even with the simplest mobile phones from customer perspective.

According to [6] in order to enhance the security in the authentication process a combination of two authentication mechanisms personal identification number PIN and Visa card, which is called two-factor authentication (2FA/TFA), can be done. Usually, 2FA/TFA involves something the user knows, for example a password and something the user has, possibly a smartcard or any other token and finally something the user "is" for example a fingerprint or voice pattern but this is not practically adopt for mobile services .

Various authors suggested various techniques to provide end-to-end security improvement for SMS. Neetesh et al., in [19] provided a framework and protocol that provide security over SMS .The Survey is based on the technique used to provide security to the SMS. Neetesh et el., in [19].This proposed protocol prevents various attacks like Man-in middle, SMS Spoofing, Replay attack, SMS disclosure.

Geovandro et al., in [20] proposed a framework for secure SMS transmission. SMS Cryptography encloses a tailored selection of lightweight cryptographic algorithms and protocols, providing encryption, authentication and signature services. For confidentiality purpose it used public key cryptography and for authentication purpose it uses block cipher based Message Authentication Code (MAC) for generating a message and key-dependent tag appended to each SMS message.

Nikhil and Mithil in [21] proposed a framework for providing end-to-end security for transmission of SMS. In this framework is used the existing GSM encryption algorithm A8 for maintaining confidentiality

The main contribution of the work of Mohsen.T et al., in [22] is introducing a new secure application layer protocol, called SSMS, to efficiently embed the desired security attributes in the SMS messages to be used as a secure bearer in the m-payment systems. SSMS efficiently embeds the confidentiality, integrity, authentication, and non-repudiation in the SMS messages.

Johnny Li-Chang Lo [23] in his work proposed a protocol, dubbed as SMS-Sec that can be used to secure SMS communication sent by Java's Wireless Messaging API. SMS Sec has a two-phase protocol with the 1st handshake using asymmetric cryptography which occurs only once, and a more efficient symmetric handshake which is used more dominantly.

Hao Zhao and, SeadMuftic in[24] implemented a new secure mobile wallet application using J2ME for convenience and security of financial mobile transactions performed by the subscribers. AES and DES are used as an encryption methods and SHA-1 2 are used to generate hashes/keys for authentication purpose. Separate authentication module, i.e., PIV is implemented as a separate java card applet to provide authentication service to all subscribers whereas Harb et al... in[25] has used symmetric and asymmetric cryptography to develop secure mobile payment application model. It is suitable for online payment transactions; provides security with minimum cryptography keys and less encryption operations.

SMS is used as a transport channel in order to send transactions to the payer. 3DES session key is used to secure SMS communication between the customer and the bank. J2ME application generates encrypted SMS having payer's confirmation and sends it to the payer's bank.

H.Mathkour et.al... in [26]proposed a new system, i.e., Secret Short Message Service (SSMS) to secure SMS message transmission on mobile network. The system can also protect the private data saved on mobile phones. In the algorithm AES Rijndeal the Secret key is embedded in cipher text using hash used to perform encryption it is used to encrypt SMS message, decryption also uses the same secret key. Encrypted secret key is used for encryption and decryption.

N.Saxena and S.Chaudhari [27]proposed a new approach that provides SMS security using encryption and digital signatures. Firstly, message is encrypted then digital signature is applied on the encrypted message. DES, AES, DSA, and RSA are used respectively in order to encrypt SMS message. Signature generation uses hash function to get message digest. DSA signature method is used to verify signatures. DES, Triple-DES, AES and Blowfish algorithms are implemented and AES is found to take less encryption/decryption time.

M.hassinen[28]has used RSA algorithm to encrypt SMS messages used in mobile commerce, whereas keys are generated using SHA-1. Private keys are restricted to mobile devices. Authentication server will then generate certificates for public keys lightweight Directory Access Protocol (LDAP) database is used to store/retrieve those certificates. These certificates are further used by mobile user to exchange encrypted SMS messages.

D.Lisonkand M.Drahansky [29]proposed an application to encrypt SMS messages using asymmetric RSA cipher. OAEP (Optimal Asymmetric Encryption Padding) scheme is used to avoid RSA from dictionary attacks. Private keys are stored in the application, whereas public keys are stored in mobile memory. Symbian OS is used as a programming environment since it requires less computational power [29]. Key generation operation is tested on Nokia N80 by subtracting the actual start time of key generation from its final time. Analysis of several attacks on application is also conducted at the end.

Alfredo De.Santiset.al...in [30]proposed a Secure Extensible and Efficient SMS (SEESMS) application framework which allows two mobile peers to exchange encrypted SMS messages in an efficient manner by selecting their level of security. ECIES (*Elliptic Curve Integrated Encryption Scheme)* and RSA are used for encryption. RSA, DSA, and ECDSA (Elliptic Curve Digital Signature Algorithm) signatures are also used to validate contacts. After being registered with SEESMS on mobile, keys are exchanged between users to transmit secure SMS using HMAC(hash based message authentication code).Users will then select energy efficient cryptosystem, encrypt SMS using it, and send to the receiver. Comparison of RSA, DSA, and ECDSA is conducted on the basis of energy efficiency on N95 mobile.

2.9 Summery

This chapter presented related works based on the set objectives of the thesis. It covered security of mobile banking on different authentication and end-to-end security mechanisms. Issues related to confidentiality, integrity, availability and authentication through different mechanism and algorithms security frameworks. There are limitations observed in the related works that are addressed by this work, Studies try to develop different authentication mechanisms to enhance security like biometric solution, voice recognition, two factor authentication and one time passwords are they are more secure than PINs but those solutions are not consider non-smart phone users and lacks user familiarity. This work proposes a model that works on all kinds of phones and without additional infrastructure.

Chapter Three

The Proposed Solution

3.1 The Proposed Security Mechanism

The proposed solution provides a mechanism for secure end-to-end mobile banking transactions. For this purpose the AES symmetric encryption algorithm is used for encryption purpose. To start using mobile banking services first, the user registers its mobile number to respected bank. The bank verifies the details of the customer and saves the mobile number in the bank's mobile banking database and gives a secured key to the customer in the format of SMS or in an email letter. The customer also fills security question and answer pairs that are provided by the bank. This secure key and customer security question and answer pairs are stored in an encrypted format in the bank's data-base.

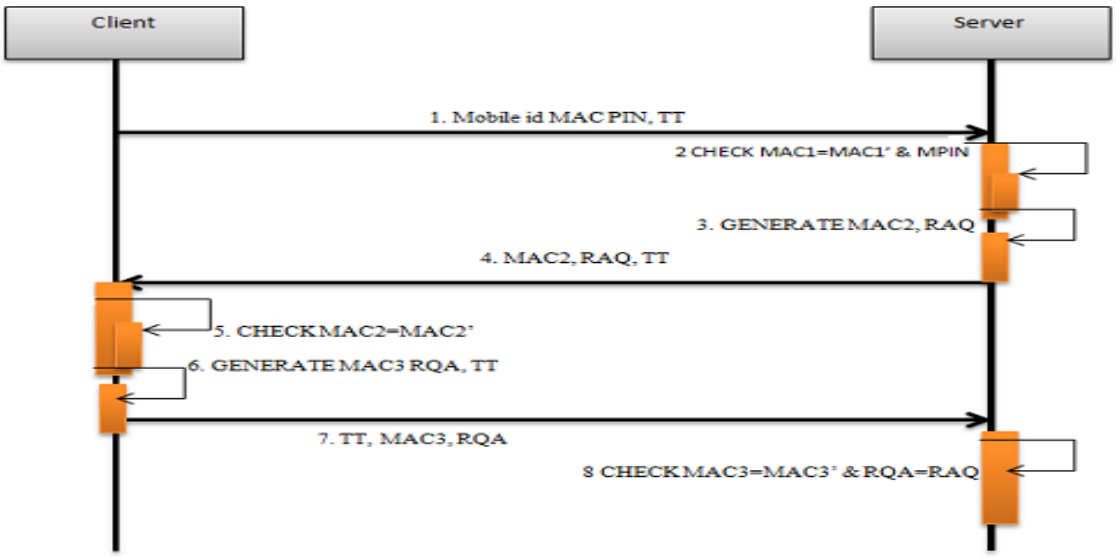


Figure 3.1: Proposed Client-Server Communication

Table3.1: Legend

MOBILE ID	Mobile Phone Identification that Registered on Network
PIN	Personal Identification Number
TT	Transaction Time
MAC1,MAC1', MAC2,MAC2',MAC3,MAC3'	Hashing Algorithm
RAQ	Random Question
RQA	Random Question Answer

The secure message contains mobile ID,,MAC (message authentication code), encrypted message and transaction time the client sends mobile id MAC1 encrypted message will be generated using AES symmetric encryption algorithm and transaction time is at the time request will be generated this all contains are send to the bank server .server decrypt the message and verify MAC1=MAC1' and check mobile id if its correct then it generate(RAQ) random question encrypted using symmetric algorithm that retrieved from the bank server .this RAQ are stored into database the server sends mac2 E(RAQ) and transaction time all these contain are send to client. The client decrypt the message and calculate MAC2' and check if MAC2=MAC2' if it's found correct it send back to E (RQA) random question answer and MAC3 and transaction time to the server the server decrypt the message and verify MAC3'=MAC3 and RAQ=RQA if it's found correct then the server sends back reply to the client server check the RAQ with the stored RQA its found correct then authentication of client is successful.

3.2 End-to-end Security

The best, easiest, and most profitable solution is to deploy the end-to-end security or security at the application layer. Most GSM security vulnerabilities (except SIM cloning and DoS attacks) do not aim ordinary people, and their targets are usually restricted to special groups so it is reasonable and economical that such groups make their communications secure using end-to-end security mechanisms. Since the encryption and security establishment is performed at the end-entities, any change to the GSM hardware will not be required. In this way, even if the conversation is eavesdropped by the police or legal organizations, they cannot decrypt the transmitted data without having the true ciphering key. Therefore, in order to avoid illegal activities, it should be transparent to both GSM operator and service provider. It may also be necessary to find solutions for a legal interception or a key screw scheme. The end-to-end security establishment has a complete flexibility to the deployed algorithms so the appropriate upgrades can be easily accomplished when necessary. However, it may be a subject to export control.

3.3 AES Algorithm

Advanced encryption standard (AES) algorithm is an encryption algorithm to maintain data confidentiality. Both hardware and software are implementations are faster still it is the new encryption standard recommended by NIST (national institute of standards and technology) to replace the digital signature based algorithm named DES[31]. According to[32], AES is more secure and efficient compared to DES and DES3. Summary of research results compared the performance of AES, DES and DES3 as shown in the Table 3.2.

Table 3.2: Comparison between AES, DES and 3DES (adopted from [35])

Factors	AES	3DES	DES
Key length	128,192 or 256 bits	(k1,k2 and k3)168 bits (k1 and k2 is same 112 bits	56 bits
Cipher type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher
Block size	128,192,or 256 bits	64 bits	64 bits
Developed	2000	1978	1977
Cryptanalysis resistance	Strong differential truncated differential ,linier interpolation and square attack	Vulnerable to differential ,brute force attacker could be analyzed a plain text using differential cryptanalysis	Vulnerable to differential and cryptanalysis; weak substitution tables
Security	Considered secured	One only weak which is exit in DES	Proven inadequate
Possible key	2^{128} 2^{192} or 2^{256}	2^{112} or 2^{168}	2^{56}
Time required to check all possible at 50 billion keys per second	For a 128-bit key:$5*10^{21}$	For a 112-bit key :800 days	For a 56-bit key :400 days

Another research result presented in [33]stated why AES is preferable over others is stated as follows:

- AES performs consistently well in both hardware and software platforms under wide range of environments this include 8-bit and 64-bit platforms.
- Its inherent parallelism facilitates efficient use of processor resources resulting in very good software performance
- It requires less memory for implementation making it suitable for restricted space environments memory constrained system like mobile phones.
- The structure has good potential for benefiting from instruction level parallelism
- There are no serious week keys in AES.
- It supports any block size and key sizes that are multiples of 32.
- Statistical analysis of the cipher text has not been possible even after using a huge number of taste case
- No differential and linier cryptanalysis attack has been yet approved on AES.

A performance comparison among AES, DES and triple DES for different micro controllers shows that AES has computational cost of the same order as required for triple DES [33].

Another performance evaluation reveals that AES has advantage over other algorithms like 3DES, DES and Ron's code2 (RC2) in terms of execution time with different packet sizes and throughput for encryption as well as decryption [34]. Moreover, in the case of changing data types such as image instead of text it has been found that AES has an advantage over RC2, Rivest cipher6 (RC6) and blowfish in terms of computational time consumption [33].

3.4Security Procedure

The developed system will not affect the existing mobile banking service that currently available. Instead it integrated with the existing system without much modification on infrastructure. The user will register for mobile banking service in a given bank branch. The branch has registration format for the service application. The format has personal questions and answers as mandatory fields used for identification.

First, authentication is performed using PIN, and then the bank side server generates a random question from its database for another confirmation. The customer is provided three attempts to try but he/she fails to provide the right information in this trials they can be blocked to consult the bank's branch.

Pre-information saved in the banks server before starting any transaction those information's can be the customer's five or more questions with his/her responses that can be, for example primary school name, birth place, memorable day, special names, wild animal or any something only person knows.

The system will use that personal questions and answers for advance authentication during a given financial transaction systematically. Firstly the system authenticates the user by personal identification number. In the developed system the PIN is changed to alpha numeric character e.g.2825 to 2A58 that will improve authentication mechanism.

After authentication of the user by his/her PIN the developed model will generate random question from the database that the person only knows. The developed model will allow the user modify the answer. Every communication with the user and server will encrypted by AES symmetric encryption algorithm to enhance end to end security it also works in any mobile phone. This is elaborated in, Figure 4.1.

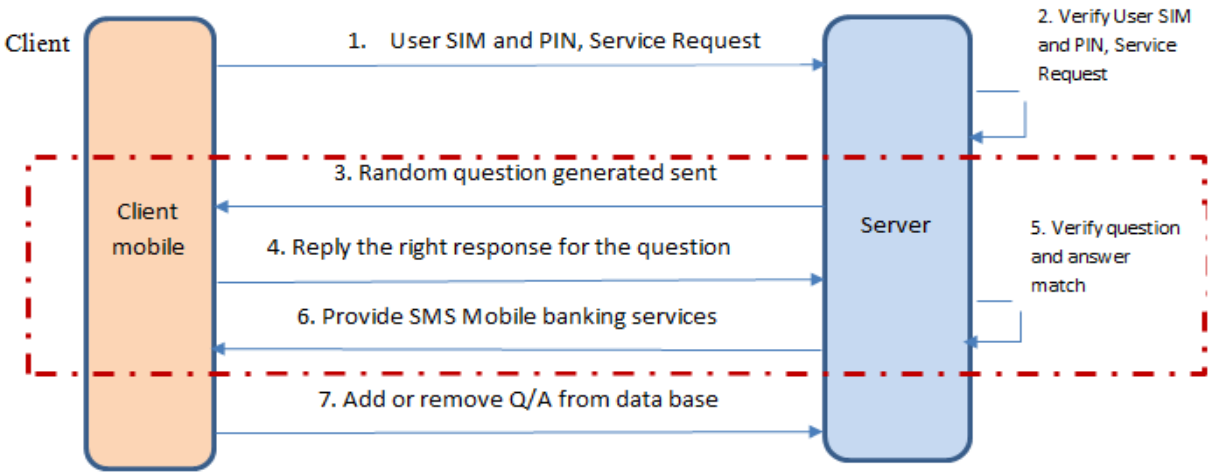


Figure 3.2: Procedure of the proposed model

The developed prototype run a number of sequential operation take place as follow

- Mobile client application prompt the user to enter USSD *889# string
- The request is sent to server side application
- Then the service responds by user PIN requisition enquiry and the user enters its PIN
- The request is sent to the server side to authenticate user identity
- The server side application will respond to the authentication process with server side initiated random question
- The user replies the question with appropriate answer to authenticate the genuine user
- The server replies with the main menu of the service
- The application let the user to modify answer on the menu option
- The server will respond to the client with the required information
- Client application shows the information to the user

3.5 Discussion

This research aimed at designing an authentication solution that is most suitable for mobile banking. Currently, PIN authentication is the most prevalent form of verification technique for mobile banking, but the background literature survey had unveiled numerous limitations related to PIN authentication. One of those limitations PIN strength for authentication, which has been investigated in many cognitive and research studies; solutions were proposed to exploit the picture superiority effect to overcome the authentication issue. Studies try to develop different authentication mechanisms to enhance security like biometric solution, voice recognition, two factor authentication and one time passwords they are more secure than PINs but those solutions are not consider non-smart phone users and user familiarity. The main focus of this work was to conform to the principles of secure service. The user is authenticated to the system using a preselected PIN which a user must give while performing any transaction on the system. Some improvements have been added by using a combination of numbers, letters and symbols to increase resistance against brute force attacks. The randomly generated user managed question and answer and the use of encryption keys also ensure that only the authorized customer can perform a transaction. Symmetric key ciphers are used to encrypt message contents in order to ensure data confidentiality. Since the keys used are known by the client side and the server side only, the communications between them will remain confidential as long as the keys remain a secret the key used for encryption/decryption is uniquely associated with only one subscriber. Since only this key can encrypt messages that will be successfully decrypted by the server, neither of the parties can deny its involvement in any transaction. Thus, the encryption key in addition to the PIN plus user managed question and answer used to hold a customer responsible for transactions performed on one's account. It is important for financial service providers to protect their communications in order to ensure secure conductance of mobile transactions.

Chapter Four

Implementation

The mobile banking channel can be delivered to the consumer through two bearer or application environments. Client-side and server-side Client-side applications are applications that reside on the consumers SIM card or on their actual mobile phone device. Client-side technologies include J2ME and S@T [35]. Server-side applications are developed on a server away from the consumer mobile phone or SIM card. Server-side technologies include USSD2, IVR, SSMS and WAP. The bank would only need to select one of these bearer channels, or bearer channel strategies, for implementation, SMS Banking requires a registered customer to initiate a transaction by sending a structured SMS (SSMS) message to the Mobile Banking Service. SSMS would be sent to SMS short code or address (a shorter version of a phone number). The SSMS would pass from the consumer's handset through the GSM Network to the SMSC (Short Message Service Centre). A SMSC stores and forwards the SSMS to the SMS Gateway allocated to the short code used by the Mobile Banking Service Provider. The Mobile Banking Service Provider would use the consumer's mobile number, forwarded by the SMSC with the SSMS, to identify the consumer and respond to the consumer's request. The response would follow the same return path.

4.1 General Structure of the Proposed Model

The proposed model is the SMS based mobile banking solution. The primary objective is to secure communications through added authentication between the mobile and the server in order to prevent any tampering on the exchanged data. The reason for adopting an SMS solution is mainly its independence with equipment manufacturers' as opposed to the USSD which requires some added features in mobile phones and/or the USSD gateway. This model is structured in three tiers; the mobile client with a C# application, the application server, and a backend database server that is integrated in the core banking system. These entities are demonstrated in Figure 4.1.

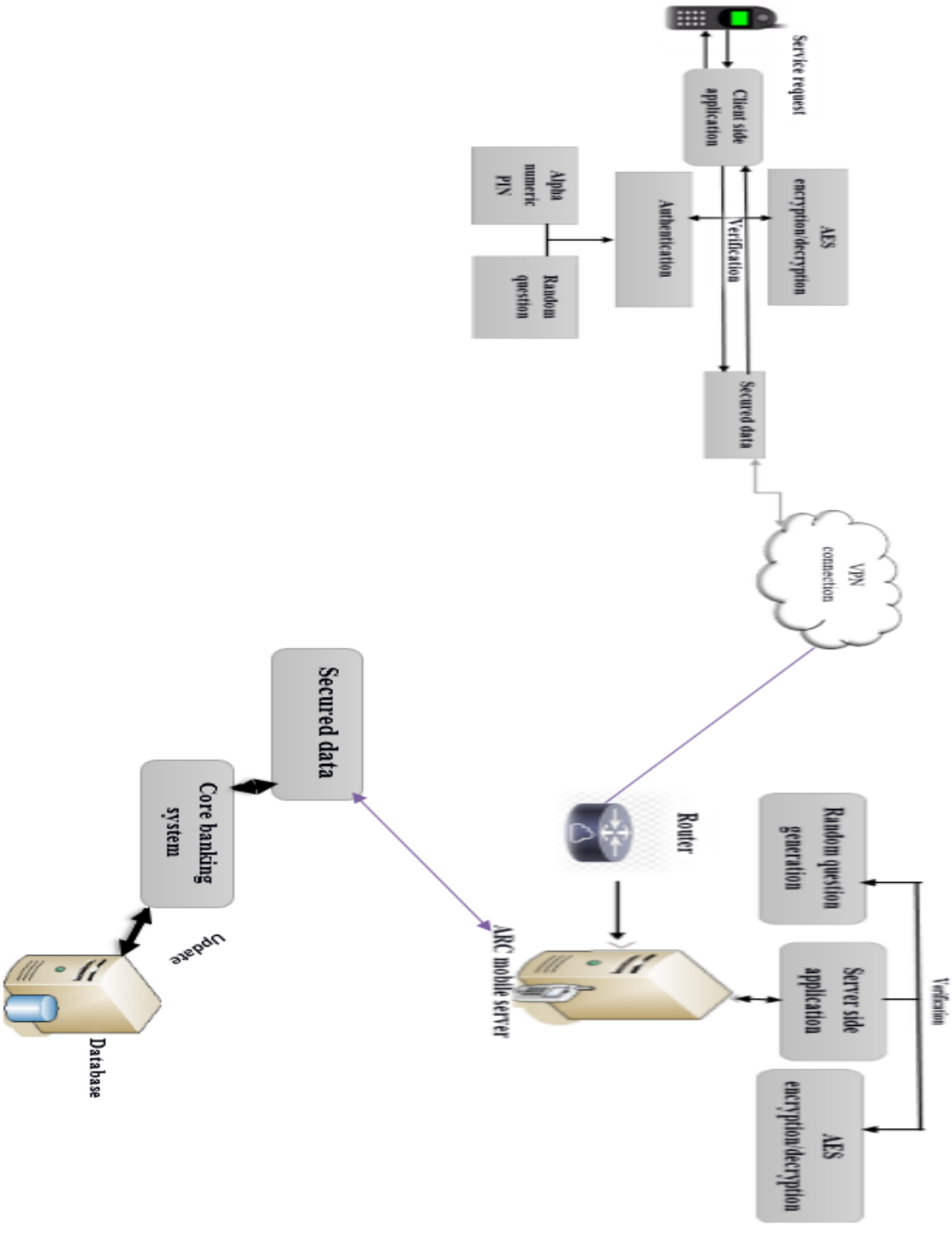


Figure 4.1 General Structure of the Proposed Model

4.1.1 The Mobile Client Application

The client mobile application resides in the customer's mobile phone and it is responsible for initiating transaction requests, capture required security details and generate a secure message. The application will then send a message via SMS across the GSM network to a server using a pre-configured SMS short code.

4.1.2 The Mobile Application Server

The server application listens on the network for incoming requests and upon receiving one; it decodes the encrypted message into some interpretable format. It then uses the designed protocol to perform the security checks on the received request before executing it. This component can be located and administered by a particular application vendor or it can be independently located and administered by the bank itself. It initiates the communication with a banking system that contains a database that has all the banking and security details of users.

4.1.3 The Backend Database Server

Customer's banking details, security details, and other related user information are kept in the database that is integrated with the core banking system. This information is utilized by the server application for customer authentication and execution of the various requested transactions.

4.2Implemented Model

The system prototype implementation model is demonstrated. NET Framework is utilized in the implementation to realize the features incorporated in the model. The prototype system structure is composed of three separate components as discussed on the structure of the system; a mobile banking application client and application server that is also running a database server. The client application is implemented by C# program running on a PC to model a mobile phone. The client cannot directly communicate with the database server but it has to go through the server application. The transaction requests are generated by the user from the client computer and forwarded to the server application. The server application responds to the client requests by communicating to the bank database server to retrieve and update the stored data.

.NET Framework was used as an Integrated Development Environment (IDE). It helps to implement various cross-platform applications. The application client was developed as a Client Application in C# using embedded library files to create executable files for deployment on a target device. The database was implemented using My-SQL database server. My-SQL connection is realized through the C# Database Connectivity (JDBC) using My-SQL connector library. Besides, the data encryption and creation of message digests are done using the security libraries included in .NET Framework. For data encryption, the Advanced Encryption Standard, AES, algorithm was used where it is suitable for devices constrained in memory capacities. It is a symmetric block cipher that uses 128 bit blocks for encryption and whose supported key sizes are 128, 192, and 256 bits. Secure Hash Algorithm 1, MAC was used to create message digests. This hashing algorithm takes a message with a maximum length of 264 bits and produces an output message of 160 bits.

4.2.1Question and Answer Random Function

The Question and Answer function is a new feature in the mobile banking system that enhances the authentication mechanism in the SMS-based mobile banking service. It is fully controlled by the user of mobile banking service at run time in addition to the PIN. The question and answer can be added, modified and deleted from the database. Hence, during every request for mobile banking service user authentication will be performed through a randomly generated number to identify which question to be asked and compare the response to pre-saved answer. Then, the server can decide whether the user is valid or not. In a way, the random number generator helps to create unpredictable question with its response answer to operate on the banking services every time a new session is requested.

4.2.2 Enhanced Authentication Measures

Authentication is meant to verify users' identities preventing unauthorized individuals from using system resources by claiming to be someone they are not. As Mobile banking is growing there are number of issues and threats in mobile banking system and the major challenge of mobile banking is users' behavior. They may lose, theft their mobile or leak login information which make others perform unauthorized operation on someone's mobile. Therefore, enhancing the customer side authentication mechanism can minimize the vulnerability to related attacks. Thus, customers can perform financial transaction or banking services feeling more confident on their mobile whenever the authentication is improved and supported by simple featured mobile above figure 3:3 elaborate enhanced mechanism diagrammatically

The propositions for enhanced authentication include:

- Having initiation question and answer will authenticate the user in something the user only knows and no one can have access even if the party has the users password or PIN
- Having the characters masked as the user types in his/her phone in order to conceal it from an eavesdropper who may be watching and later attempt to perform a masquerade attack.
- It can also strengthen the PIN by allowing it to contain characters other than numbers (a combination of numbers, letters, and symbols is proposed). This will improve the current PIN which constitutes of 4 digits number only.

Every user or mobile banking client should have a minimum of 5 pairs of additional fields with their login user name (SIM information) and PIN.

Any user can have a maximum of 10 pairs of question and answer fields on the authentication database which also help to identify (authenticate) the client every time he/she requests for mobile banking services.

The user can add or remove questions and answer pairs from the database by using main menu where the users can change it as they wish and three trials is allowed but on the third unsuccessful trial the server provides a reply that the user is blocked from SMS mobile banking services. Then, the server will inform to contact the nearby branch of the bank to renew the service again.

Chapter Five

Prototype Testing and Evaluation

5.1 Overview

In this chapter, testing and evaluation of the improved security mechanisms and the developed prototype will be discussed. In this study; an SMS based solution has been designed and its prototype has been implemented to address the security issues that are associated with conducting mobile banking transactions over GSM. For enhanced security measures in mobile transactions; data need to be encrypted and provisions to ensure message integrity have to be enforced prior to sending the message over the network. This is for the purpose of ensuring end-to-end security of data between the customer and the financial institution. And also, improvements are made for securing authentication mechanisms that are applied currently in Ethiopia by adding additional authentication measures. Henceforth, the testing and evaluation of these security mechanisms will commence.

5.2 User Validation and Security Challenge on the New System

This section has analyzed the prototype of the proposed system in terms of the features of the system that user's desire. This analysis is done by making available the new system to some user groups; make them use it exploiting the various features of the new system and by collecting their responses through interviews and discussions.

A series of steps will deploy to check the security of randomly generated question and try to guess the user PIN through user1 and user2.

Step1 what if the user supplies the correct value

- The system allows the user to dial *889#
- The user enters PIN
- Responds the randomly generated question through correct value
- Uses banking services

Step 2 what if the user supplies incorrect value

- The user forgot one character of the PIN
  - ✓ Allows three trial for unless the system informs the user to contact the bank branch
- User forgot the randomly generated question
  - ✓ the system allows two trials the system informs the user to contact the bank branch
- Both users try to guess each other's PIN
  - ✓ The system blocks the user1 through more trials
- Deliberately user1 has user2's PIN to guess the randomly generated questions
  - ✓ The system blocks the user ID through wrong answer

It is possible to see that the proposed system here performs much better than the old system. In analyzing the proposed system for possible security flaws, based on the analysis made on the four criteria a system must meet before it is deemed secure. These criteria include user/server authentication, confidentiality, data integrity and non-repudiation. User/Server authentication according to the users test results the new system fulfills the expected criteria.

5.3 Testing and Evaluation

In this sub-section end-to-end and random question and answer authentication features of the improved mobile banking security system is tested and evaluated to ensure the proposed solution can enhance end-to-end and authentication mechanisms. Usability was considered during the design and implementation of the mechanism but the main concern of this work is security.

5.3.1 Confidentiality of AES

The level of security of the designed algorithm depends on the strength of the encryption algorithm used. The type of algorithm needed for this project is symmetric key encryption algorithm. The algorithm must perform encryption relatively fast in the mobile phone environment. Therefore the AES algorithms were considered to perform the message encryption. NSA (national security agency) no15 has conducted a review and analysis of using AES to protect classified information. AES is an NSA approved cryptographic algorithm to be used for United States national security information and system at all classification levels [36]. The use of 128 bits key length is approved to be sufficient to protect classified information up to the US national secret level.

The speed of encrypting a message depends on the size of the original message. Since the designed mechanism uses SMS to transmit secure details, therefore the upper bound of the size of the original message cannot exceed the size of an SMS message which is 160 characters. The second testing for confidentiality is that the encrypted message can be decrypted. Since we are using symmetric key encryption, we must be able use the encryption key to decrypt the message.

5.3.2Authentication

The authentication question and answer mechanism is only known by the user only any attackers cant guess the exact pair of randomly generated question additionally authentication detail (PIN) of the user is protected within the encrypted banking details. The attacker cannot read the authentication detail of the user therefore the attacker cannot use the authentication detail to perform masquerading attacks.

5.3.3 Brute Force Attack

If the user gets hold of the transmitting message, it is possible for the attacker to crack the cipher message to read the security details; therefore secure algorithms are needed to ensure message contents are protected. The strength of the banking details protection depends on the strength of the encryption algorithm and the strength of encryption keys generation. If we assume the attacker uses brute force attack to try crack the message content, then the following calculation shows how much time the attacker needs to crack the message.

We assume the keys are purely random. The following sets of characters are allowed to be in the generated key: [a-z] size = 26, [A-Z] size = 26, [0-9] size = 10.Therefore the possible characters size is 26+26+10 = 62.If the attacker uses an advance computer to perform the attack and it can process 10^6decryptions per second. The key size is between 8 to 16 characters (any keys that are less than 16characters are padded with space characters). Therefore the attacker has to try 62^8+ 62^9+ 62^{10}+ 62^{11}+ 62^{12}+ 62^{13}+ 62^{14}+ 62^{15}+ 62^{16}= 4.845 x $10^{28.}$ And we further assume on average it would take the attacker half the number of tries to before he/she cracks the message content. Therefore after2.422 x 10^{28}tries the attacker can read the message content.

The average number of years that requires the attacker using brute force attack to crack the encrypted message would be 2.422 x 10^{28}years/10^6 x 60 x 60 x 24 x365.25 = 7.677 x 10^{14}years

The above calculation shown that on average, it is computationally infeasible for the attacker to use brute force attack to crack the encrypted message.

5.4 Summary

Secure SMS banking mechanism can be designed and implemented that offers better security. The designed mechanism can enhance the required authentication and end-to-end security features? The designed protocol can be integrated with mobile banking to form secure SMS banking?

There are many security problems with the current GSM architecture and its SMS protocol. The main security concern is that if the user wants to send sensitive data using SMS, the message can be intersected. A third person from the cellular service provider with authority can read or alter the content of the message. Therefore the security of the message is compromised. This work provides designed secure SMS banking security mechanism. The mechanism ensures the transmitting SMS message is secure and the message can be delivered to the destination securely it conforms to the principles of security service. The implementation follows the secure SMS protocol to transfer and receive mobile banking messages. In this work security algorithm which covers the security shortfalls of the standard SMS protocol and the protocol was designed to follow the principle of security service. The security algorithm is can be integrated with a mobile banking solution without affecting the current banking service. Authentication mechanism also enhanced through alphanumeric password that isn't easily captured by eavesdroppers and also added random question and answer mechanism tested through other users on developed prototype by telling the users PIN to guess the randomly generated questions of other user in those testing scenarios; the designed security mechanism was proven secure than current SMS banking security mechanism.

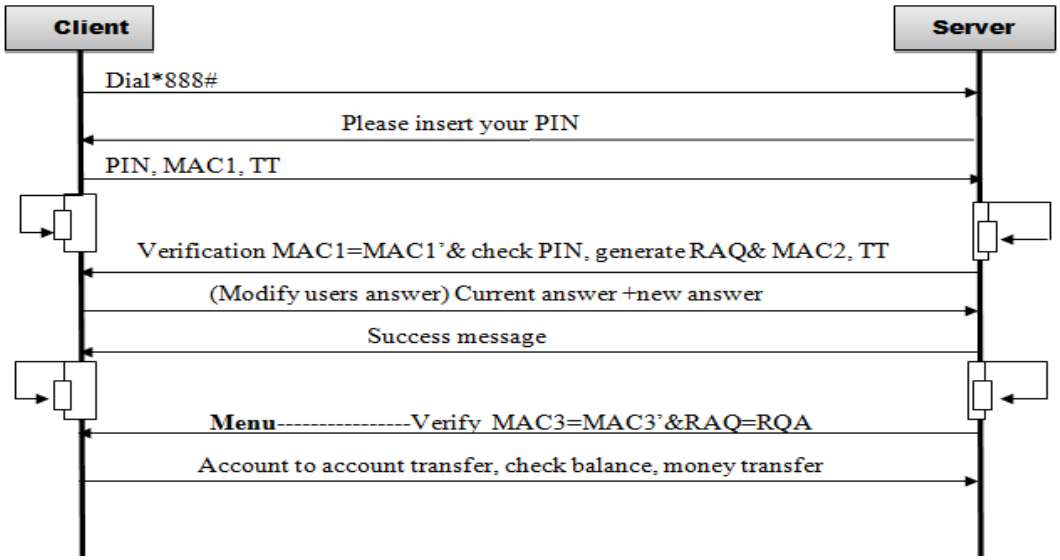


Figure 5.1Developed Security Mechanism Scenario

5.5 Security Analysis

The main focus of the design goals for the model was to conform to the principles of secure service. These are user authenticity, confidentiality of data, non-repudiation, data integrity, and availability of service. There are security concerns that can be mentioned on any security framework this constraints are confidentiality integrity authenticity this work maintain those constraints.

5.5.1User Authentication

The user is authenticated to the system using a pre-selected PIN which a user must give while performing any transaction on the system. Some improvements have been added by using a combination of numbers, letters and symbols to increase resistance against brute force attacks. Random question authentication also ensures that only the authorized customer can perform a transaction.

5.5.2Data Confidentiality

Symmetric key ciphers are used to encrypt message contents in order to ensure data confidentiality. Since the keys used are known by the customer and the bank only, the communications between them will remain confidential as long as the keys remain a secret.

5.5.3Non-repudiation

The key used for encryption/decryption is uniquely associated with only one subscriber. Since only this key can encrypt messages that will be successfully decrypted by the server, neither of the parties can deny its involvement in any transaction. Only the customer and the bank should have knowledge of the key; all successful transactions, therefore, must have originated from a customer with a correct key. Thus, the encryption key in addition to the PIN can be used to hold a customer responsible for transactions performed on one's account.

5.5.4Integrity

Message digests are used to ensure message integrity where hashes of message contents are calculated at both ends and then compared. If the digest calculated by the sender differs from that generated by the receiver; the recipient will detect a compromise in the message integrity.

Table 5.1: Comparison between Existing vs. Proposed Approaches.

Existing Approaches	Proposed Approach
Current USSD technology sends its data in clear text across GSM	Proposed model utilizes SMS based solution that encrypts data between the client and server
No mechanisms for message integrity checking in existing system	Message are checked for integrity at the receiving end using message digest
The current PIN vulnerable to eavesdroppers attack	Use combination of numbers and at least one alphabet to construct PIN
The current authentication measures is less secure for financial service	Implement additional security enhancement mechanism after PIN requisition
Current system works only one language	Has additional local languages for usability

Figure 5.2: Proposed System Prototype – User Entering a PIN

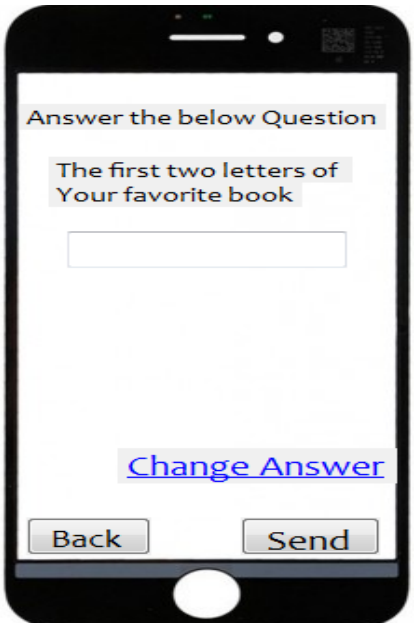


Figure 5.3: Random Question and Answer Authentication Mechanism

Chapter Six

Conclusions and Future Works

6.1 Conclusions

SMS communication isn't yet fully secure and hence it is not generally trustworthy. To place trust on SMS messaging especially if it is used in an enterprise environment, a protocol should be in place to ensure confidentiality, integrity and authentication between the two communicating parties. The simple password access control on the application interface is not enough to assure security. An enhanced security model for mobile banking systems has been presented in this paper. The model incorporates enhanced security controls to be used in securing transactions. On this study, the requirements for the proposed model were identified, the model was then designed and its prototype has been implemented. Thus, it is important for financial service providers to protect their communications to and from customers in order to ensure secure mobile transactions. This work fills this need by implementing various security controls to the current system; the messages are encrypted, and hash codes are utilized to guarantee message trustworthiness. The authentication mechanism has been improved as related to user managed random question and answer mechanism. The model can thus be used to securely conduct mobile transactions over unsecured channels. Hence, in this thesis work the enhancement of the authentication mechanism of mobile banking and the end-to-end security of mobile banking systems are done. The proposed solution provides all the necessary security mechanisms to perform a secure mobile banking transaction.

6.2 Future Works

There are still several issues regarding the security of mobile banking that warrant further research. The focus for future works could be to implement and test the proposed model in real environment setting, to explore efficient and effective ways to improve security of transactions carried by USSD technologies. Moreover, testing with different security threats and measuring the performance could be taken as another dimension. Besides, a feasibility analysis need to be conducted on the use of future mobile communication systems for conducting mobile transactions along with its security implications. The proposed model can be applied to agent banking services that are currently applied in Ethiopia like CBE-birr, M-birr, Oro-birr and Awash-birr because they can hold huge financial transactions.

References

[1] Mobile thinking, 2013. [Online]. Available: http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers.. [Accessed 15 March 2017].

[2] Reporter, "Ethiopian telecomunications corporation mobile subscription," Addisababa, 2017.

[3] "wikipedia," [Online]. Available: https://en.m.wikipedia.org/wiki/Mobile_banking.. [Accessed 15 july 2017].

[4] C. Dermish, "Mobile banking solutions for the poor," vol. I, no. 2, pp. 1-33, 2011.

[5] Emmanuel and B.jacobs, "Mobile banking in developing countries," redbound university nijmegn, 2011.

[6] C.chong A.arnab and ChikomoK, "Security of mobile banking," 2006.

[7] T. a. A.beheshti, "solution to the GSM security weakness," in *next generation mobile application services and technology*, 2006.

[8] Reporter, "National bank of ethiopia directives," Addisababa Ethiopia, 2017.

[9] M. Alemu, "cloud computing security framework for banking industry," 2013.

[10] V. Merwe, "Mobile commerce over GSM," *banking perspective on security,* 2003.

[11] Strasburg.J, "online banking grows," 2015.

[12] R. security, RSA security consumer study reveals major concerns over online security, 2006.

[13] C. networks, analisis reveals usage of online banking and bill payment, 2006.

[14] FFIEC, "authentication in internet banking environment," 11 february 2006.

[15] M.karen and A.beheshti, "solution to the GSM security weaknesses," in *next generation mobile application*, 2008.

[16] T.takada and H.koike, "image-based authentication for mobile phones using users fevorite images," 2008.

[17] Medhi.A, "comparision of mobile money-transfer UI's," 2009.

[18] Chong.MK, "usable authentication for mobile banking," jun 2009.

[19] N.saxena,S.neetesh and S.chaudhary, "aprotocole for end-to-end secure transmission of SMS," *transaction on information forensics and security,* vol. 4, 2014.

[20] C.preeira,AMateus and D. C.geovandro, "alightweight cryptographic framework for secure SMS transmission," *journal of systems and software ,* 2013.

[21] M. Nikhil Sakhare, "secure system for SMS on GSM networks," *international journal of soft computing and artefcial intelegence ,* 2013.

[22] A.Mohsen Toorani, "secure SMS messaging protocol for M-payment systems," 2008.

[23] Lo.j Bishop and j.H.Elo, "end-to-end protocol for secure SMS," *computers and security,* vol. 27, pp. 154-167, 2008.

[24] H.Zhao and S. Muftic, "desigen and implementation of mobile transactions client system," *international journal for information security research ,* vol. 1, pp. 113-120, 2011.

[25] H.Harb, H.Farahat, and M. Ezz, "secure SMS mobile payment model," in *anti-counter feiting security and identification ASID*, 2008.

[26] H.Mathkour, G.Assassa, A. Al-Muharib, and A. Jumah, "asecured criptographic messaging system," in *machine learning and computing(ICMLC)*, 2009.

[27] N.saxena,S.neetesh and S.chaudhary "secure encryption with digital signature approach for SMS," in *world congress on information and comunication technology(ICMLC)*, 2012.

[28] M.hassinen, "Java based public key infrastructure for SMS messaging," in *confrence on information and communication technologies*, 2006.

[29] D.lisonek and M.Drahansky, "SMS encryption for mobile communication technologies," *security technology SECTECH08,* pp. 198-201, 2008.

[30] A. De Santis, A. Castiglione, G. Cattaneo, M.Cembalo, F. Petagna, and U. F. Petrillo, "an extensible framework for secure SMS," in *complex intelegent and software intensive systems (CISIS)*, 2010.

[31] KawserWazedNafi1 and Dr.M.M.AHashem,"anewer user authentication ,file encription and distributed server based architecture," 2013.

[32] Mahajan,prerna and A.sachdeva "study of encryption algorithm AES,DES,RSA for security," in *computer science and technology*, 2013.

[33] B. Hamdan.O.Alanazi, "new comparative study between DES,3DES,and AES within factors," *journal of computing,* vol. 2, 2010.

[34] Punithasurya and S.jebapriya, "analisis of different access control mechanism in cloud," *international journal of applied information systems,* 2012.

[35] Nyamtiga.B, "security perspectives for USSD versus SMS in conducting mobile transactions," 2013.

[36] Commite on national security. system, "CNNS policy factsheet no1," USA, 2006.

Appendix A

Questionnaires'

1. Do you own a mobile phone?

   (a) Yes, which model? (b) No

2. Do you have a bank account?

   (a).Yes, which bank do you bank with? (b)No

3. Do you bank with mobile banking?

   (a).Yes (b) No why?

4. Did you think m-banking is secure enough?

   (a).Yes (b) No why?

5. Did you thing current m-banking service is user friendly (easy to operate)?

   (a).Yes (b) No what makes it difficult?

6. How long do you normally leave you phone switched on?

   (a) Always on (b) Switch phone off at night (c) Switch phone off during weekend

   (d) Only switch phone on when it is needed (e) others

7. Do you trust your mobile phone for communication security?Trust that other people cannot access the information on your phone?

   (a) .Yes, what makes you trust your phone? (b) .No, why?

8. How often do you do banking?

   (a) Daily (b) Weekly (c) Once in 2 Weeks (d) Monthly (e) Once in 2 Months

9. What do you do with a bank account? (Can select multiple options)

   (a) Check Balance (b) Withdraw Cash (c) Account Payment (d) Buy Airtime

   (e) Shopping (f) Transfer Money (g) others, please specify

10. Do you trust banks? E.g. Do you trust that you money will not be stolen from your bank account?

    (a) Yes, Why? (b) No, Why?

11. Do you have access to the internet?

    (a) Yes, do you use internet banking (e-banking)? (b) No

12. Do you trust internet banking?

    (a) Yes, why? (b) No, why?

13. Do you trust banking with your mobile phone?

    (a) Yes, why? (b) No, why?

14. Did you think that the banks have to work on m-banking security and usability?

    (a) Yes, why? (b) No, why?

Open questions

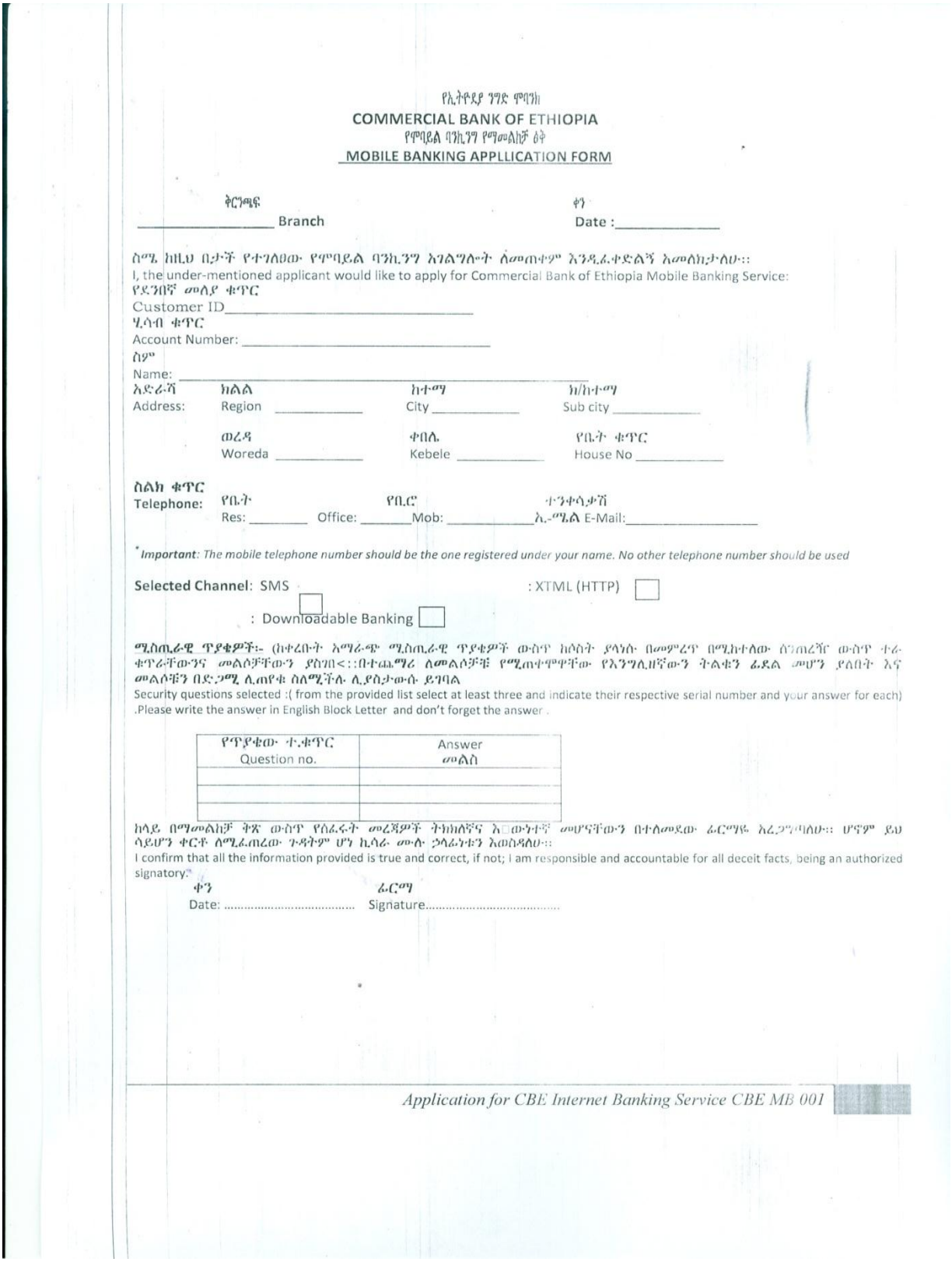
1. What was your attitude towards mobile banking security?

---

2. What makes you not to use m-banking service?

Appendix B

Current mobile banking application format



የኢትዮጲያ ንግድ ባንክ
COMMERCIAL BANK OF ETHIOPIA
የሞባይል ባንኪንግ የማመልከቻ ፅቅ
MOBILE BANKING APPLLICATION FORM

ቅርንጫፍ _____ Branch
ቀን Date :_____

ስሜ ከዚህ በታች የተገለፀው የሞባይል ባንኪንግ አገልግሎት ለመጠቀም እንዲፈቀድልኝ አመለክታለሁ።
I, the under-mentioned applicant would like to apply for Commercial Bank of Ethiopia Mobile Banking Service:
የደንበኛ መለያ ቁጥር
Customer ID_____
ሂሳብ ቁጥር
Account Number: _____
ስም
Name: _____
አድራሻ Address: ክልል Region _____ ከተማ City _____ ክ/ከተማ Sub city _____
ወረዳ Woreda _____ ቀበሌ Kebele _____ የቤት ቁጥር House No _____

ስልክ ቁጥር
Telephone: የቤት Res: _____ የቢሮ Office: _____ ተንቀሳቃሽ Mob: _____ ኢ-ሜል E-Mail:_____

*Important: The mobile telephone number should be the one registered under your name. No other telephone number should be used

Selected Channel: SMS ☐ : XTML (HTTP) ☐
: Downloadable Banking ☐

ሚስጢራዊ ጥያቄዎች፡- (ከቀረቡት አማራጭ ሚስጢራዊ ጥያቄዎች ውስጥ ከሶስት ያላነሱ በመምረጥ በሚከተለው ሰንጠረዥ ውስጥ ተራ ቁጥራቸውንና መልሶቻቸውን ያስገቡ<:::በተጨማሪ ለመልሶቻቹ የሚጠቀሟቸው የእንግሊዘኛውን ትልቁን ፊደል መሆን ያለበት እና መልሶቹን በድጋሚ ሊጠየቁ ስለሚችሉ ሊያስታውሱ ይገባል
Security questions selected :(from the provided list select at least three and indicate their respective serial number and your answer for each) .Please write the answer in English Block Letter and don't forget the answer .

የጥያቄው ተ.ቁጥር Question no.	Answer መልስ

ከላይ በማመልከቻ ቅጽ ውስጥ የሰፈሩት መረጃዎች ትክክለኛና እውነተኛ መሆናቸውን በተለመደው ፊርማዬ አረጋግጣለሁ። ሆኖም ይህ ላይሆን ቀርቶ ለሚፈጠረው ጉዳትም ሆነ ኪሳራ ሙሉ ኃላፊነቱን እወስዳለሁ።
I confirm that all the information provided is true and correct, if not; I am responsible and accountable for all deceit facts, being an authorized signatory.

ቀን Date: ..... ፊርማ Signature.....

Application for CBE Internet Banking Service CBE MB 001

Appendix C

Commercial Bank of Ethiopia
Mobile Banking Service
SECURITY QUESTIONS

1) WHAT IS YOUR FAVORITE COLOR?
የሚወዱት የቀለም ዓይነት?

2) WHAT IS YOUR SPOUSE NAME?
የባለቤ□ስም ማን ትባላለች/ይባላል?

3) WHAT IS YOUR GRAND MOTHER'S NAME?
የሴት አያቶ ስም ማን ይባላል?

4) WHAT IS THE NAME OF YOUR FIRST CHILD?
የመጀመሪያ ልጅዎ ስም ማን ይባላል?

5) WHAT IS THE NAME OF YOUR BIRTH PLACE?
የተወለዱበት አካባቢ ምን ተብሎ ይጠራል?

6) WHAT IS THE NAME OF MUSICIAN THAT YOU ADMIRE MOST?
የሚያደንቁትድምፃዊ ስም ማን ይባላል?

7) WHAT IS THE NAME OF THE BRIDGE THAT YOU CROSS FREQUENTLY?
አዘውትረው የሚያቋርጡበት ድልድይ ስም ማን ይባላል?

8) WHAT IS YOUR ELEMENTARY SCHOOL NAME?
የመጀመሪያ ደረጃ ትምህርት የተማሩበት ት/ ቤትስም ማን ይባላል?

9) WHAT IS THE NAME OF UNIVERSITY/COLLEGE THAT YOU ATTENDED?
የተማሩበት ዩኒቨርሲቲ/ኮሌጅ መጠሪያ ስም ማን ይባላል?

10) WHAT IS THE NAME OF YOUR YOUNGER SISTER?
የታናሽእህትዎስም ማን ይባላል?

11) WHAT IS THE NAME OF YOUR YOUNGER BROTHER?
የታናሽ ወንድምዎ ስም ማን ይባላል?

12) WHAT IS THE NAME OF YOUR ELDER SISTER?
የታላቅ እህትዎስም ማን ይባላል?

13) WHAT IS THE NAME OF YOUR ELDER BROTHER?
የታላቅ ወንድምዎ ስም ማን ይባላል?

14) WHAT IS THE NAME OF THE CHURCH THAT YOU WORSHIP IN MOST?
አዘውትረው የሚሄዱበት ቤ/ክርስቲያን መጠሪያ ስም ማን ይባላል?

15) WHAT IS THE NAME OF THE MOSQUE THAT YOU WORSHIP IN MOST?
አዘውትረው የሚሄዱበትመስጊድ መጠሪያ ስም ማን ይባላል?

16) WHAT IS YOUR Most FAVORITE TRADITIONAL FOOD?
ክባህላዊ ምግቦች ውስጥእርስዎ በጣም የሚወዱት የትኛውን ነው?/አንዱን ብቻ ይግለፁ

17) WHAT IS YOUR BEST FRIEND'S NICK NAME?
የቅርብ ጓደኛዎ የቅፅል መጠሪያ ስም ማን ይባላል?

18) THE FIRST CITY OR TOWN YOU START JOB?
መጀመሪያ ስራ የጀመሩበት ከተማ መጠሪያ ስም ማን ይባላል?

Mobile Banking Application Summary Form CBE- IBS -002