Conceptual Security Framework for Mobile Banking Key Authentication and Message Exchange Protocols: Case of Ethiopian Banks

A Thesis Presented

by

Betelhem Belete G/Hiwot

to

The Faculty of Informatics

of

St. Mary's University

In Partial Fulfillment of the Requirements for the Degree of Master of Science

in

Computer Science

July, 2017

ACCEPTANCE

Conceptual Security Framework for Mobile Banking Key Authentication and Message Exchange Protocols: Case of Ethiopian Banks

By

Betelhem Belete G/Hiwot

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:

Mr. Asrat Beyene

Internal Examiner

Dr. Engineer Yhenew Woldea(PhD)

External Examiner

Mr. Asrat Beyene

Dean, Faculty of Informatics

July 8, 2017

DECLARATION

I, the undersigned, declare that this thesis is my original work, has not been presented for a degree in this or any other universities, and all sources of materials used for the thesis work have been duly acknowledged.

Betelhem Belete G/Hiwot

Studet

Addis Ababa

Ethiopia

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

Dr. Henock Mulugeta

Advisor

Addis Ababa

Ethiopia

July 8, 2017

ACKNOWLEDGMENTS

First and foremost I am grateful to God, who kindly helped me to complete my thesis. Then I would like to express my special appreciation and thankfulness to my advisor, Dr. Henock Mulugeta for his continuous support, patience, motivation, enthusiasm, and immense knowledge.

I would like to thank the expert and professionals at Commercial Bank of Ethiopia, Nib International Bank and Bank of Abyssinia for their invaluable assistance they have provided me during the process of information gathering and analysis. My research would not have been possible without their help. Special thanks goes to my family, my beloved husband, friends and subordinates for their continuous support and encouragement with their best wishes towards my goal, without whose love, encouragement, and prayer I would not have finished this thesis.

Table of Contents

LIST OF ACRONYMS

ATM	Automated Teller Machine
AVR	Automated Voice Response
BSC	Base Station Controller
BTS	Base Transceiver Station
CBE	Commercial Bank of Ethiopia
DDOS	Distributed Denial of Service
E-Banking	Electronic Banking
E-Payment	Electronic Payment
GSM	Global System for Mobile Communication
HLR	Home Location Registers
JASA	Java Application Security Architecture
ISC	International Switching Center
ICT	Information & Communication Technologies
IMSI	International Mobile Subscriber Identity
IT	Information Technology
IVR	Interactive Voice Communication
LAI	Location Area Identity
LSM	Light Weight Security Mechanism
MFSP	Mobile Financial Service Providers
MNO	Mobile Network Operator
MSC	Mobile Switching Center
NIB	Nib International Bank

PC	Personal Computer
PDA	Personal Digital Assistant
PFM	Personal Financial Management
PIN	Personal Identification Number
PKY	Public Key Interface
POS	Point of Sale
SMAC	Standalone Mobile Application Clients
SIM	Subscriber Identity Module
SMS	Short Message Service
SMSC	Short Message Service Center
TIMSI	Temporary International Mobile Subscriber Identity
VLR	Visitor Location Registers
WAP	Wireless Application Protocol
WIG	Wireless Internet Gateway
WWW	World Wide Web

LISTS OF FIGURES

LISTS OF TABLES

ABSTRACT

Many people are using their mobile devices such as smart phones to access various online services on a daily basis. In particular, mobile banking applications are increasingly becoming popular. Despite popularity however, there seem to be some very genuine concerns on the security issues revolving around it, particularly in regard to man in the middle attacks.

Many banks in Ethiopia are offering mobile banking services which allow bank customers to check balance in their personal account and to transfer money between accounts at any time by simply using mobile banking applications installed on their mobile devices. According to the survey analysis we made all banks in Ethiopia implementing Mobile Banking services we motivated to facilitate some security landscapes focusing only on the bank - side and believed that customer - side security is up to the customer to worry about. However, it has been identified that the major security threat is social engineering and its loopholes are customer - side security related. The current situation observed in the Ethiopian Banking industry is that the technology of mobile banking applications are far from totally clean and mature.

This research demonstrates that there is a strong pressure on mobile banking application developers to take care of not only users' privacy but also the banks security. The result of this research will help Ethiopian banks to revisit their focus of attention in constructing and implementing customer side security to reduce from man – in - the - middle attacks logically tied to this channel of banking service. It is shown that, the functionality of the proposed framework will help to reduce risk scenarios for mobile banking key authentication and message exchange protocols.

Key words: **Mobile Banking, Security framework, E-Banking, Man in the middle attack, Authentication, Key Message exchange**

CHAPTER ONE

INTRODUCTION

1.1. Overview

The fast advancing global information infrastructure (including information technology and computer networks such as the Internet and telecommunications systems) enable the development of electronic commerce at a global level. ICT are playing a very important role in the advancements in banking. In fact ICT are enabling banks to make radical changes to the way they operate [1].

E-banking can mean the provision of information about a bank and its services via a home page on the World Wide Web (WWW). A more sophisticated Internet based service provides the customer with access to their accounts, the ability to move money between different accounts, make payment or apply for loans and other financial products [2].

Innovative banking has grown since then, aided by technological developments in the telecommunications and information technology industry. The early decade of the 1990s witnessed the emergence of Automated Voice Response (AVR) technology. By using the AVR Technology, banks could offer telephone banking facilities for financial services. With further advancements in technology, banks were able to offer services, through PC owned and operated by costumers at their convenience, through the use of intranet propriety software. The users of these services were, however, mainly corporate customers rather than retail ones. The security first network bank was the first Internet banking in the world that was built in 1995 in USA. After that some famous banks introduced their internet banking one after another, such as Citibank and bank of America [1].

E-banking largely came into picture as a result of technological developments in the field of computing and communications but there have been a number of other factors or challenges which played an important part in its development. First, they need to satisfy customer requirements that are complex and ever changing. Second, they need to deal with increased competition from old as well as new entrants coming into the market. Third, they need to address the pressures on the supply chain to deliver their services quickly. Finally, they must continually

develop new and innovative services to differentiate themselves from the competition, as having a large branch network is no longer seen as a main source of competitive advantage e-banking is seen by many banks as a key tool to address these challenges [2].

The rapid growing information and communication technology is knocking the front door of every organization in the world, where Ethiopian banks in general would never be exceptional. In the face of rapid expansion of 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 [3]. Technological innovations play a crucial role in banking industry by creating value for banks and customers, that it enables customers to perform banking transactions without visiting a brick and mortar banking system. On the other hand E-banking has enabled banking institutions to compete more effectively in the global environment by extending their products and services beyond the restriction of time and space [1]. However, mirroring the development of E-commerce, the adoption and diffusion of E-banking system is not well developed in Ethiopia.

1.2. Background of the study

Modern banking in Ethiopia was introduced in 1905. At the time, an agreement was reached between Emperor Menelik II and a representative of the British owned National Bank of Egypt to open a new bank in Ethiopia. February 15, 1906 marked the beginning of banking in Ethiopia history when the first Bank of Abyssinia was inaugurated by Emperor Menelik II [3].

Immediately after the enactment of the proclamation private banking companies began to flourish, leading to 16 private banks and 2 public owned commercial banks which are Development Bank and Commercial Bank of Ethiopia operating in Ethiopia [3].

The appearance of E-banking in Ethiopia goes back to the late 2001, when the largest state owned, Commercial Bank of Ethiopia (CBE) introduced Automated Teller Machines (ATMs) to deliver service to the local users. Despite being the pioneer in introducing ATM based payment systems and acquired visa membership, CBE lagged behind Dashen Bank, which worked aggressively to maintain its lead in E-payment systems. As CBE continues to move at a snail's pace in its turnkey solution for Card Based Payment system, Dashen Bank remains so far the sole player in the field of E-Banking since 2006 [4]. By the end of 2008 Wegagen Bank has signed an agreement with Technology Associates (TA), an Ethiopian based information

technology (IT) firm, for the development of the solutions for the payment system and installation of a network of ATMs on December 30, 2008.

The Ethiopian banking business is moving towards the modern banking services with the implementation of information technologies. In the most recent years, the introduction and implementation of Internet Banking, Mobile and Agent Banking, and Card Banking services are some of the major products and services being implemented at some banks [4].

Mobile banking may be described as the newest channel in electronic banking to provide a convenient way of performing banking transactions using mobile devices. The potential for mobile banking may be far greater than typical desk-top access, as there are several times more mobile phone users than online PC users. Increasingly "mobile life styles" may also fuel the growth of anywhere, anytime applications [2].

There are two main types of technologies available for use in mobile Banking: Wireless Application Protocol (WAP) and Wireless Internet Gateway (WIG). WAP is an application environment and set of communication protocols for wireless devices designed to enable manufacturer, vendor, and platform independent access to the Internet and advanced telephony services. WIG is an SMS-based service, in which a menu of available banking options is initially downloaded from the bank to the phone device. This enables users to browse bank accounts and conduct other banking related tasks [2].

Mobile banking brings new opportunities and risks to financial providers, carriers and the financial system. On the one hand, it holds out the prospect of adding new convenience for accessing banking and payment services to existing banked customers. Especially, in developing countries, it may go even further to offer banking and payment services to those who have never participated in the formal electronic banking system before. In the process, banks, Mobile Network Operator (MNO) and third party suppliers stand to gain. These opportunities have caused new players to enter this market [2].

On the other hand, the addition of a new channel brings new operational risks to providers, just as the introduction of Internet banking more than a decade ago opened new categories for risk. For this reason, Mobile Financial Service Providers (MFSP) seeking to enter the market, or those already in the market, has to assess their risks and develop strategies to mitigate them on an ongoing basis. As adoption of mobile financial services increases, financial regulators in various

countries are also paying increasing attention to the specific risks brought by the use of the mobile channel [5].

A Key area concern for consumers and financial service providers is the security of mobile banking and payments. There are new technologies and new entrants as well as a complex supply chain that will increase the security risks. There is no real standard for technology that has captured the market and regulations relative to some of the new entrants are non-existent. Customers have increased control of their device in terms of application downloads, operating system updates and personalization of their devices. These will lead to new challenges relative to privacy and will take some time before the younger generation realizes the implications of privacy violations. Compounding the challenges is the fact that traditional security controls such as AV, firewalls, and encryption have not reached the level of maturity needed in the mobile space.

As with any emerging market area, these challenges will resolve over time. Until these get mature, there are measures that can be taken relative to customer education, service process rigor, payments

technology and fraud preventive and detective controls that can mitigate the security risks [4].

1.3. Research Motivation

After of the fall of the Derge Regime, immediately there was an enactment of the proclamation that allows private banking companies to flourish, leading to sixteen private banks and two public owned commercial banks which are Development Bank and Commercial Bank of Ethiopia operating in Ethiopia (As the number of Banks increase and the introduction of information which leads to the transformation of conventional bank to E-Banking). Almost all Banks are in fierce competition by introducing Internet, Mobile and Card Banking to attract their customers. One of their competition ground is Mobile Banking Services as all group of the society own Mobile Devices.

However, banks did not enjoy the fruit of their investment on Mobile Banking Services, because of adoption problem of the general public. This emanate from the biggest security issue raised by customer. Thus, these scenarios motivated us to work and contribute on Mobile Banking security issue, especially from the customer's side.

1.4. Statement of the Problem

Mobile banking has been widely used in developed countries and is rapidly expanding in developing countries [3]. Ethiopia's financial sector remain behind in expanding the use of the technology with a growing number of Mobile users and in the meantime the growing availability of Mobile Banking services create security vulnerabilities in line with lack of language, the current Mobile Banking system is short of availing security protection from the customer side.

Therefore, the purpose of this paper is to identify the main security challenges of customers to use the existing mobile banking applications which are offering in many government and non-government banks of Ethiopia, and improve the existing security framework which can increase the trust of customers in using the technology and minimize the security risks in the customer side.

1.5. Research Question

The following research questions are formulated to address the research problem:

- What mobile banking security mechanisms of the customer's side are currently applied in the Ethiopian Banking industry?
- What are the main concerns of customers for using the existing mobile banking technologies which are implemented by Ethiopian Banking industry?
- What are the drawbacks of the current security mechanisms in the customer's side?
- How can we address the drawbacks and security concerns, which increase the customers trust in using the technology?

1.6. Objectives

1.6.1. General Objective

The general objective of this research is to use multi-factor authentication security framework for Mobile-Banking Key Authentication and Message Exchange protocol for the Ethiopian Banking industry context.

1.6.2. Specific Objectives

- To review current M-Banking applications in Ethiopia Banking industry;
- To assess the current M-Banking security mechanisms in customers side applied by Ethiopian Banking industry;
- To propose a Mobile-Banking Key Authentication and Message Exchange protocol applicable to the Ethiopian banking industry and
- Evaluate the new security framework.

1.7. Scope and limitation of the study

Considering the objective of the study, this thesis aimed to enhance Mobile Banking security framework of customers side for banking industry and research have been conducted based on primary data collected from customers of the largest bank in Ethiopia which is state owned bank called Commercial Bank of Ethiopia (CBE) and professionals from CBE and private banks called Nib International Bank (NIB) and Bank of Abyssinia and IT experts in private owned ICT company called BeabIcT Solutions – BITS. Those Banks are selected as a sample, because of that all Banks in Ethiopia are using same type of Mobile Banking application and applying same type of security mechanisms.

Elaboration of the limitation

- Lack of security experts and companies in the country makes the study difficult.
- Non-existence of such kind of research before affects the study, due to lack of appropriate experience.
- The time constraint of the study force to take the proof of concepts only in one bank.
- For the sake of information security, some of the Bank's information was kept confidential; hence data collection is limited.

1.8. Significant of the study

The major contribution of this study is to propose a security framework of M-Banking key authentication and message exchange protocols, and enhancing the framework to support the typical banking industry in Ethiopia. This will benefit Banks to offer more secured M-Banking services of customers - side to the market, increase the number of customers using the M-Banking technologies and protects customers from hackers and third party access to their account information.

1.9. Organization of the study

The research report is organized into six chapters: Chapter one focuses on the background of the study, problem statement, objectives and significant of the study. In Chapter two, a range of literatures review is captured there to gather relevant information concerning mobile banking security issues. In chapter three, detail of methodology followed to achieve results is outlined. It includes the study design, sampling and sampling technique. Chapter four contained the proposed security framework for mobile banking key authentication and message exchange protocols, which are the main security issues of Ethiopian bank customers. Chapter five evaluates the proposed conceptual framework. Chapter six focus on main findings, conclusion and recommendations of the study.

CHAPTER TWO

LITERATURE REVIEW

2.1. Overview

This chapter presents a review of related studies and major concepts and capabilities enabling technologies for mobile banking and their inherent security limitations. The Global System for Mobile communication network (GSM) functionality and its security deficiencies is discussed here. The GSM is the data transmission media in the SMS protocol and the flaws in its architecture have led to the security shortfalls in SMS-banking system. It is therefore important to provide an overview of its architecture [6]. The GSM technical specification elaborates the architecture of the GSM system. The specification was started in 1982 by the European conference of postal and telecommunications administrations (CEPT) [7]. The GSM system offers the user the ability to be mobile. The subscriber identity module (SIM) is used for purposes of authentication. It gives the network operator on whose behalf the SIM has been issued the complete control over all subscription and security issues.

2.2. Concepts in Mobile Banking Technology

Mobile banking can be broken into three key areas: Informational, Transactional and Service, Marketing and Acquisition. Within the area of informational there are functions such as balance and transaction history, loan, mortgage, and credit information, ATM and branch locators, as well as personal financial management (PFM) functions such as spending comparisons with peers or budget tools. Transactional services included account transfers, bill pay, person to person payments and remote deposit capture. Service features included functions that enhance the customer's experience including contact options, help information, and alerts. Additional service features include product renewal notifications, balance triggered savings offers, balance triggered credit offers, and location triggered travel insurance options. Finally, relative to marketing and acquisition, there are services such as mobile coupons/incentives, barcodes, new product information, customer research, cross selling and acquisition. The aspects of mobile that make it particularly appealing to marketing are the very personal nature of mobile devices and the "always on" aspect of customer use [8].

2.2.1. Global system for mobile communication

Global System for Mobile communications (GSM) is a cellular network, which means that mobile phones connect to it by searching for cells in the immediate vicinity. GSM networks operate in four different frequency ranges. Most GSM networks operate in the 900 MHz or 1800 MHz bands. Some countries in the Americas use the 850 MHz and 1900 MHz bands because the 900 and 1800 MHz frequency bands were already allocated. The rarer 400 and 450 MHz frequency bands are assigned in some countries, where these frequencies were previously used for first-generation systems. GSM is a globally accepted standard for digital cellular communication. It is the name of a standardization group established in 1982 to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz [9].

2.2.2. GSM Architecture

This section briefly describes the functionality of the various components illustrated in figure 2.1. The GSM comprises of various components in the figure the solid lines show communication between core components. The dotted lines show the internal connection for communication used during maintenance. In a typical communication operation the Mobile Station (MS) which is in effect a cellular handset initiates the communication. The communication signals are transmitted from the MS and received by the Base Transceiver Station (BTS). The function of the BTS is to receive and transmit radio signal to and from the MS. It is also responsible for translating the radio signals into digital format and transferring them to the Base Station Controller (BSC). The BSC forwards the received signals to the Mobile Switching Centre (MSC). The MSC interrogates the Home and Visitor Location Registers (HLR and VLR) this databases keep location of the destination MS. In the event that the received signal is an SMS message then it is routed to the Short Message Service Centre (SMSC) for delivery to the required destination. The SMSC keeps a copy of the sent SMS in its database after it has been sent. In case of an international connection the signal is routed through the International Switching Centre (ISC). In order to facilitate equipment verification and user authentication the Equipment Identity Register and Authentications Register database are used. The operation and management center controls maintenance operations [6].

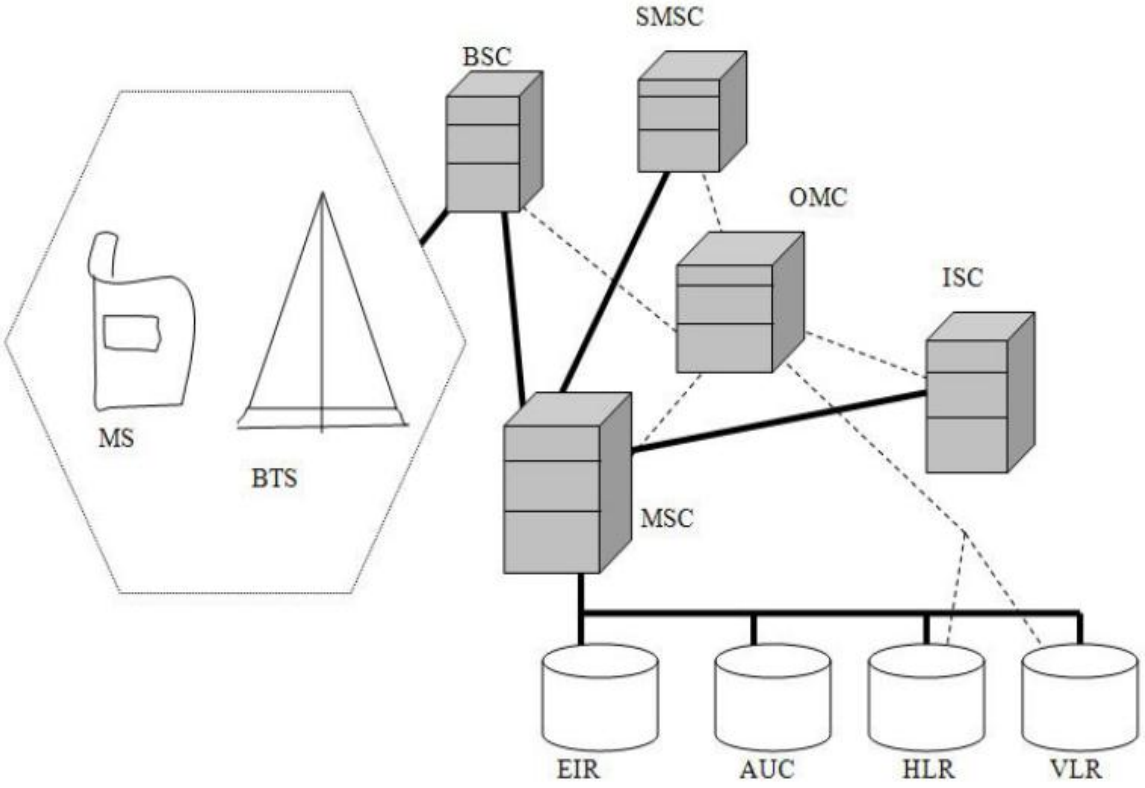


Figure 2.1: GSM Architecture [6].

Key: Giving Full Meanings of GSM Architecture Component Abbreviations

MS – Mobile station,
BTS – Base Transceiver Switch,
BSC – Base Station Controller,
MSC– Mobile Switch Centre,
ISC – International Switching Centre,
VLR- Visitor Location Registry
EIR–Equipment Identity Register
AUC– Authentication center
HLR – Home Location Registry
SMSC–Short Message Service Centre
OMC– Operation Management Centre

2.2.3. GSM Security

In order to protect network operators and users the GSM system specification provides implementation of a number of security features. The following features are taken from the perspective of the user.

- Subscriber identity confidentiality
- Subscriber identity authentication
- User data confidentiality

2.2.3.1. Subscriber Identity Confidentiality

The GSM system uses temporary identities to deny an intruder the possibility of gaining information on the resources used by a subscriber for example preventing the tracing of user's location and matching a user with the data transmitted [10]. The system uses the International Mobile Subscriber Identity (IMSI) number to uniquely identify subscribers. The identity is stored in the Subscriber Interface Module (SIM) card issued by the mobile network service provider. The mobile cellular phone operates only with a valid SIM. During subscriber verification it is desirable to keep the subscribers IMS in numerical secure in order to prevent the adversary from localizing and tracking the user's physical location. To achieve this instead of transmitting the IMSI in plaintext a temporary IMSI is used called TIMSI [10].

The TIMSI is valid per session of subscriber verification and it is unique within each location area where the user moves. The Location Area Identity (LAI) is always used in conjunction with the TIMSI. The TIMSI, IMSI and LAI are securely stored in the VLR database of the mobile network service provider. In order to establish subscriber identity the service provider uses the IMSI of the subscriber to interrogate the VLR database for the subscribers TIMSI. The service provider compares the TMSI with the mobile phones IMSI for authentication. The TIMSI is first encrypted before it is sent over the air. Following a successful authentication the server at the service provider sends the next TIMSI to the subscriber mobile set for the next authentication [10].

2.2.3.2. Subscriber Identity Authentication

Subscriber authentication is of major interest to each operator. Its purpose is to protect the network against unauthorized use thus preventing masquerading attacks [10].The protocol utilizes a challenge response authentication mechanism. Authentication of subscriber identity is achieved using a subscriber's authentication key K_in addition to the IMSI. The key is installed in the SIM card and pre-stored in the Authentication Centre (AUC) by the service provider. The algorithm used for authentication is A3 and it requires both the subscriber's mobile phone and service operator to have the same key K_i. In order to perform an authentication the mobile network provider generates a random number (RAND) that is used to calculate the signature response (SRES). This random number is sent to the mobile subscriber's phone as well and it calculates the signature response (SRES) using this number and sends it back to the service provider. If the two SRES values are Identical the authentication is considered successful figure 2.3 illustrates the basic flow diagram of subscriber authentication.

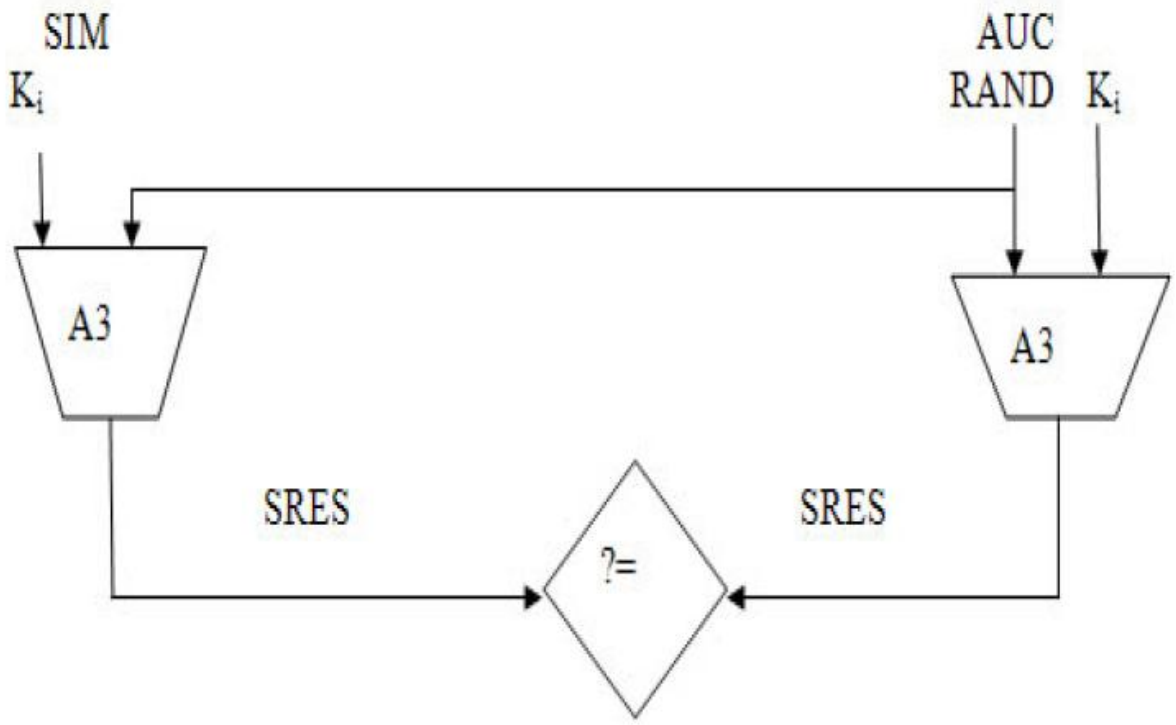


Figure 2.2: Authentication Procedure [7].

2.2.3.3. User Data Confidentiality

To ensure the privacy of user information carried in both traffic and signaling channels is upheld, the GSM system employs the A5 algorithm for encryption of transmitted data. The activation of this service is controlled by the mobile network service provider. It is initiated by the base station by sending a command to the subscriber mobile phone [11]. The A5 algorithm is a symmetric ciphering algorithm and uses a key K_c to generate a key stream that is *XO Red* with a block of plaintext to generate the cipher text. The key is derived in the SIM using the A8 algorithm generator specific to a network operator and also the RAND and *Ki* used in subscriber authentication procedure Figure 2.4. The ciphered text is converted to radio signals by the mobile phone and sent across the air to the base transceiver station. The figure below illustrates the flow diagram of cipher key generation and enciphering.

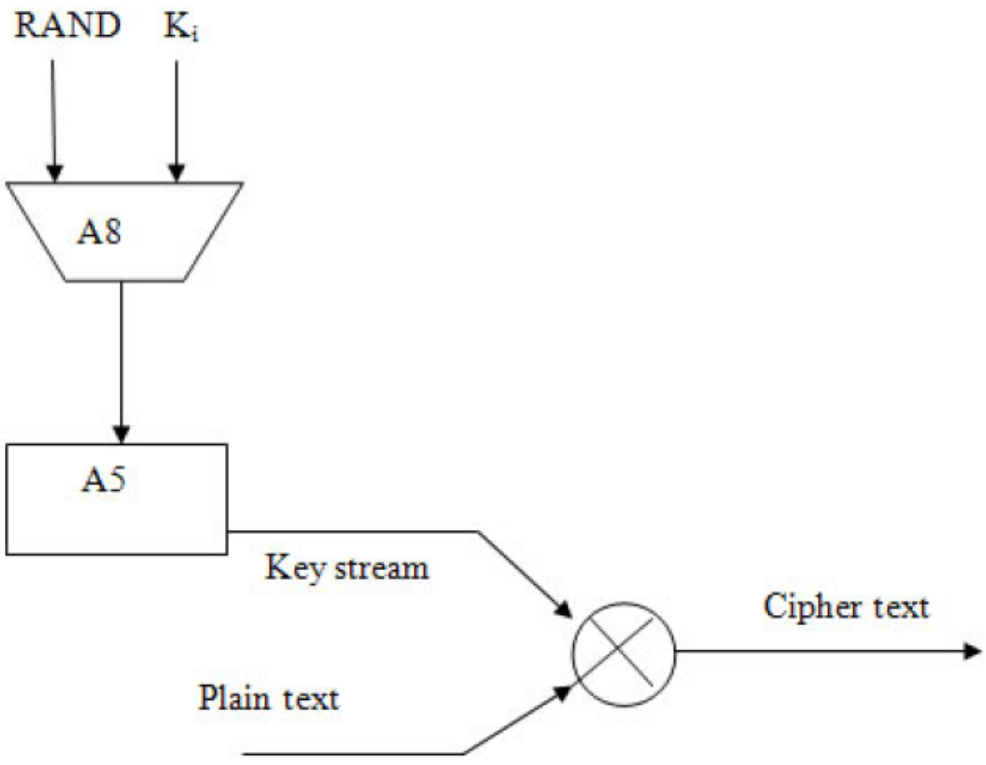


Figure 2.3: Cipher Key Generation and Enciphering [7].

2.2.4. Security Deficiencies of GSM Architecture

Much as GSM system strives to make a provision for security services as discussed in the previous sections it still has limitations in its security, it point out the lack of data integrity in the GSM. On top of this the following cryptographic issues with regard to the authentication and encryption algorithms have been identified [12].

2.2.5. A5 Encryption Algorithm

The commonly used A5 algorithm for encryption in the GSM system has already been reverse engineered [13]. The A5algorithm has two main variants A5/1 and A5/2. And there are three possible attacks on the A5/1 version that is commonly used in Europe. The attack could be achieved with a personal computer in a few seconds. The A5/2 variant was also cracked in less than a day [13]. This shows how the GSM system is vulnerable to cryptanalysis attacks.

2.2.6. A3/A8 Authentication Algorithm

The A3/A8 algorithm is a commonly used authentication algorithm throughout the world in GSM systems. A3/A8 algorithm can be broken after sporting several flaws in the algorithm. They were able to obtain the key *Ki* hence making SIM cloning feasible [16].

2.2.7. Enabling technologies for Mobile Banking

The current channels through which mobile banking services are deployed is discussed here under. Here we point out the short comings of each in relation to the others. These banking services may include any of the following;

- Credit/Debit Alerts.
- Minimum Balance Alerts.
- Bill Payment Alerts.
- Bill Payment.
- Recent Transaction History Requests.
- Information Requests like Interest Rates/Exchange Rates.
- Account Balance Enquiry
- Cheque Book Request
- Fund Transfer between Accounts.

2.2.8. Mobile Banking Operation

A mobile banking system comprises a mobile banking unit and a data processing center which may be the mainframe computer of the bank responsible for processing banking transactions and data storage. [15]

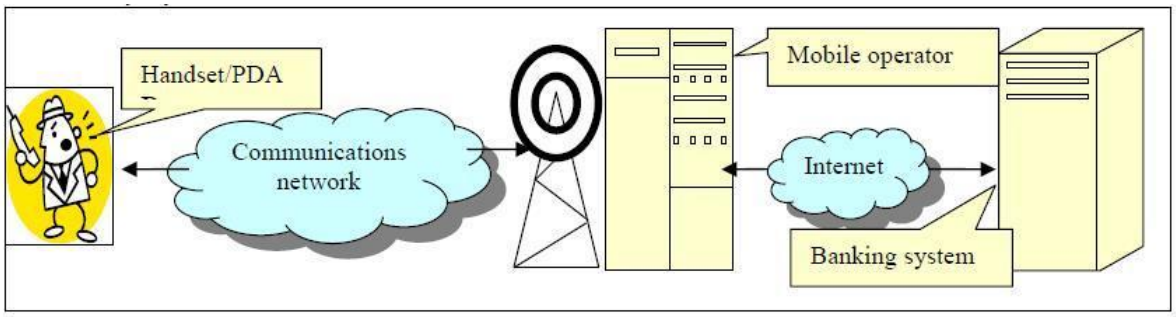


Fig 2.4 Mobile Banking Operation System [15]

Mobile banking is seen to be an extension of the existing payment infrastructure of a bank to Mobile phones as a channel for the leveraging of the mobile network and its reach, to deliver Banking services to consumers. The mobile banking infrastructure thus sits in a similar technical environment to the banks ATMs, POS, branch and internet banking service offerings.

Thus a bank's core banking system, the system that houses the consumer's account and related transaction management would translate banking instructions received from consumer through their mobile channel. The mobile banking channel can be delivered to the consumer through two bearer or application environments.

Client–side applications: are applications that reside on the consumers SIM card or on their actual mobile phone devices. Client-side technologies include J2ME and S@T.

Server-side applications: are developed on a server away from the consumer mobile phone or SIM card. Server-side technologies include USSD2, SSMS and WAP. The Bank would only need to select one of these bearers.

- USSD (Unstructured Supplementary Service Data): In its simplest definition, is a menu driven form of SMS where a customer would receive a text menu on their 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.

- WAP: is best described as the Internet on a mobile phone. It is an open international standard for applications that use wireless communication. Its principal application is to enable access to the Internet from a mobile phone or PDA. A WAP browser provides all of the basic services of a computer based web browser but is simplified to operate within the restrictions of a mobile phone
- USSD2 it would be held in the same session and allow for a flowing conversation between the user and the service. This is similar to e-mail and instant messaging, e-mail waits for the recipient to read and respond while as instant messaging allows for immediate dialogue. USSD is as standard a feature as SMS and is available in an estimated 95% of handsets today
- SSMS – when SMS Banking requires a registered customer to initiate a transaction by sending a structured SMS (SSMS) message to the Mobile Banking Service [15].

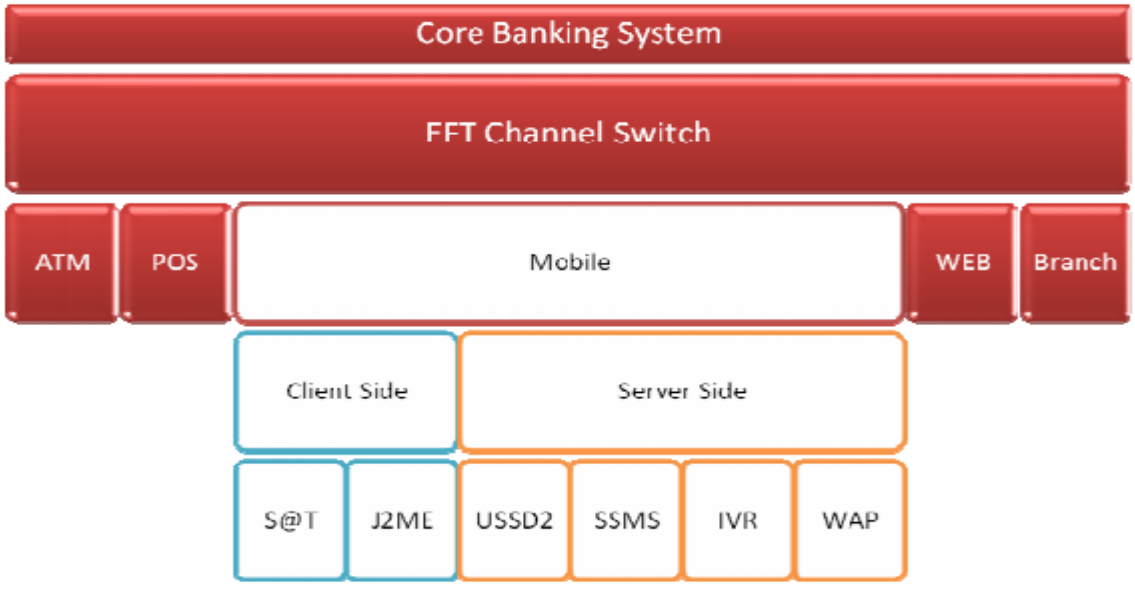


Fig. 2.5 Mobile Banking in the overall Banking architecture [15]

2.2.9. Types of risks associated with Mobile Banking

Using mobile phones for mobile banking, customers can access their bank account. It means that the customer is interacting with files, databases etc..., of the Bank. Database at the server end is sensitive in terms of security. And from customer end, if the customer loses his/her mobile phone then there is no assurance that there is a safety in using current mobile banking authentication mechanism. There are two security zones in mobile banking, one is the handset held by user and the bank security zone [12].

The following two elements contribute to a different risk environment for Mobile Banking relative to other E-Banking channels which are: the mobile handset, which comes with a wide range of functionality from basic on standard handsets to advance on feature phones and smart phones. The mobile network, which includes all the links carrying a data message from a handset to the Bank or vice versa and the methods used to communicate b/n the handset and the Bank [12] [15].

A. Distributed Denial of service (DDOS) Attack

DDOS is the most common attack of banking system. DDOS attack orbit they attack to target system. Before an attack is happen attacker will be attack network by scanning open ports.

B. Malware

Malware is the term for maliciously crafted software code. Moreover, it is possible to perform the following operations for this type of malicious software Account information theft.

- Fake web site substitution
- Account hijacking

C. TCP/IP Spoofing

An attacker gains unauthorized access to a mobile device or a network by making it show up that a malicious message has come from a trusted machine by spoofing the IP address of that machine.

D. Backdoors

Access to mobile program that avoided security mechanisms is a backdoor. A programmer may sometimes install a back door so that the program can be accessed for troubleshooting or other purposes. Back doors have been used by attackers to install themselves, as chunk of an exploit.

E. Tampering

It is an international modification of products in a way that would make them harmful to the consumer.

F. Exploits

It is a piece of software or a data which acts as a bug or vulnerability in order to matter surprising behavior to exist on computer software or hardware.

G. Social Engineering and Trojans

Trojans act as no authorized programs, can delete, block, modify and copy data.

Generally the key risks on Mobile Devices are included:

- Malware
- Malicious applications
- Privacy violations relative to application collection and distribution of data
- Wireless carrier infrastructure
- Payments infrastructure/ecosystem
- SMS vulnerabilities
- Hardware and Operating System vulnerabilities
- Complex supply chain and new entrants into the mobile ecosystem
- Lack of maturity of Fraud tools and controls

2.2.10. Mobile Banking Applications

The main types of existing mobile banking applications are the following as described in [16].

A. WAP Banking

The function of WAP banking is in many ways similar to the function of Electronic banking using http. The client sends a request and gets a response with page content which is stored on or dynamically generated by a standard web server. The main difference is in the usage of a WAP gateway for the conversion of the protocols. WAP gateway encryption protocol is converted from SSL/TLS to WTLS with the effect that data is not encrypted while it is processed while authentication is assured via a personal identification number (PIN) of the user; authorization for transactions is realized via transaction numbers (TAN) [16].

B. SMS Banking

The Short Message Service (SMS) is a GSM service to exchange text messages up to 140 byte (or 160 characters of 7 bit). The transmission of mobile-originated short messages is carried out by the short message service center (SMSC) of the particular network operator. The SMSC is receiving the message from the mobile device and routing it to the destination device. For generating mobile-terminated short messages, it is possible that a company or a special service provider runs an own SMSC. Thus, a bank could generate SMS from bank data like account balance or account movements and send it to the mobile device of the customer. The customer has to include a PIN for authorization in every SMS he sends to his bank [16].

C. Mobile Banking with PDA

A personal digital assistant (PDA), also known as a handheld PC, or personal data assistant, is a mobile device that functions as a personal information manager. The term evolved from Personal Desktop Assistant, a software term for an application that prompts or prods the user of a computer with suggestions or provides quick reference to contacts and other lists. The communication between the bank and the mobile device is typically carried out via binary SMS. Binary SMS contain in contrast to pure text SMS binary data in an 8-bit format. The usage of binary SMS is offering the possibility to secure the data against unauthorized access. The function of the access is similar the one at the SMS-banking. A SMS with customer is generated by the SMS-Gateway and sent to the mobile phone of the customer. The SMS-Gateway of the bank must be able to generate binary SMS and to encrypt them for transmission. The data which should be sent to customer is split into single data packages which are packed into single SMS [16].

D. Mobile Banking with SIM - Toolkit

SIM Application Toolkit (SIM-Toolkit, SAT) is a GSM standard for extended communication between the SIM card and the mobile device. A respective solution is storing the mobile banking application on the SIM Card of the user. On the SIM-card, several data is stored, e.g. for the authorization of customers, personal settings like phonebook entries and sent and received SMS. In addition to this, there is free storage space left for individual applications. The bank sends bank a binary SMS as an answer; the mobile phone recognizes the binary data and forwards the data for processing to the application on the SIM-Card which again uses the phone display to communicate with the user [16].

2.2.11. Requirements of Mobile Banking Applications

The requirements can be discerned into four categories: technical, usability, design and security:[16]

A. Technical Requirement

- ✓ The usage must be possible with both kinds of available mobile devices. This requirement is resulting from the characteristic that usage will be made with a mobile device.
- ✓ The application should automatically detect the kind of device it is executed on and adapt automatically to its features.
- ✓ The usage must be possible for any customer and the amount of transmitted data should be as small as possible.

B. Usability requirement

- ✓ The possibility to work offline with the application. It should be possible to use the application without a permanent connection to the bank server.
- ✓ A simplified method of data input. This requirement is of special interest when a necessity is given to enter higher amounts of data.
- ✓ Resumption of usage at the same point after disruption. This requirement is resulting from the characteristic that mobile usage can be disrupted at any time. In such a case the application should allow the user to resume his usage at same point where it was disrupted, without a complicated log-in procedure

C. Design requirement

- ✓ The possibility to personalize the application. If the user gets a lot of data displayed, there should be the possibility to use a personalized structure to view the data.
- ✓ The possibility to scale the application. This concerns the easy switch of use cases for the user, e.g. if he gets an unexpected account balance and wants to find out more details. In these cases, it should be easily possible to switch to a version of the application with a wider range of functions.
- ✓ The possibility to get announcements on important events.

D. Security requirement

- ✓ The transmission of the data has to be encrypted. This is resulting from the fact that a mobile banking application is transmitting sensitive data. To secure this data, the connection must be encrypted.
- ✓ Before usage, access to the data must be authorized. Before a user can access his data he has to prove that he is entitled to do so.
- ✓ The authorization has to be simple. Especially in the first two use cases, where a quick access to the data is important, authorization has to be fast and simple.

2.2.12. Available Security frameworks for Mobile Banking

Authentication is the process of determining whether someone or something is, in fact who or what it is declared to be. It is one of the most important security imperatives in verifying the identity of a customer and determining whether he is permitted to access a particular banking account. The traditional way of authenticating per today depends on three factors that could be something you have, something you are and something you know. The authentication process could include one of the factors or a combination of them all [13] [17] [23].

A. Something the user knows

Methods based on something the user knows are often associated with a password, multiple passwords, or a combination of a password and a username. The user has usually chosen a password before he/she starts using the service. This same password has to be provided by the user for every future use of the service [13] [17] [23].

- **Stationary computer approach**

In computer-security systems this is the most common method for authentication of users. For

most of web applications and services password authentication presents well enough solution. Even though this authentication mechanism does not provide high level of security, it is very easy for implementation, and user is usually free to choose password that is simple for him/her to remember.

- **Mobile device approach**

Based on the success of password authentication on stationary devices, the same approach has also been adopted and used on mobile devices. The first example you can see when you turn on your mobile phone. The first thing that usually happens is that you are prompted for the PIN code, before you can start using your mobile phone. On that manner the user is authenticated to the mobile network, and he/she is protected from loss and theft of the mobile device.

- **Security level**

Security level provided by this approach is not very high. There are numerous of attacks that can jeopardize user's confidentiality and security. Some of the attacks are: brute force attacks where an attacker try to log in to the service with every possible password until he/she succeeds, dictionary attack where an attacker try only passwords from the previous prepared lists, rainbow attack that present more sophisticated version of dictionary attack where passwords are hashed before and these values are used for attacks. Additionally, more threats can emerge due to improper storage of the passwords provided by the user at the time of registration.

One major problem with password and security is user factor. In most cases user is required to choose password that he/she will use on the system and remember it. The password that is chosen can greatly influence security of the user, and because of that it is very important for user to choose a strong password. On the other hand if the user is forced to choose a complicated and inconvenient password there is another problem with writing it down and forgetting it.

- **Usability issue**

We saw that authentication using passwords provide really low level of security. But also we said that this approach is very popular and widely accepted for stationary and mobile device. The biggest reason for this is high usability and easy implementation. For the user, it is required to remember password that he/she choose, but there is no complicated and demanding authentication process and privacy issues.

B. Something the user has

User authentication in this case is based on something that user has, a physical object. An object could be a mobile device or a token. Using this approach, a user is not required to reveal any private information about him/her (like in biometrics) nor is it required remembering some secret information (password) [13] [17] [23].

Stationary device approach

A token could be a small physical device that is often used to authenticate on a website or a similar services. They are used to prove one's identity electronically, and they exist in different sizes and shapes, and are often small devices that can easily be carried around. Tokens can store different kind of data that is often implemented in a chip and can perform various authentication methods. The four types of tokens are: static passwords, synchronous dynamic passwords, asynchronous passwords and challenge response. The tokens could work as standalone, or they can be connected to a computer using the USB mechanism or some kind of wireless technology like Bluetooth. The mobile phone itself can also be used as a token for user authentication for services and applications on stationary devices.

Mobile device approach

This approach for user authentication is especially suitable for authentication of a user for mobile applications and services. The biggest reason for this is that mobile device is usually considered as private device that belong just to one person, and because of that is ideal example of "something the user has". In this manner, the mobile device is functioning as both the terminal providing the service as well as the user authentication token.

There is couple of possibilities how this authentication method can be implemented on mobile devices. The biggest difference lies in how a user's private authentication information is stored or delivered to the mobile phone. The possible approaches are:

- Private information is stored on hardware (e.g. SIM card),
- Private information is stored on the specific file on the mobile device´s file system, and
- Private information is received through mobile service operation (SMS message).

Authentication of the user based on private information stored on a SIM card is usually used by network operator to authenticate subscribers. This approach provides very high level of security because user's private information is stored on tamper resistant cards. For this reason, this

approach is becoming more and more popular for authentication of the user for different mobile services (e.g. mobile banking). The biggest disadvantage is that all changes and additions to SIM cards must go through a network operator.

Authentication of the user based on private information stored on mobile device's memory is not dependent on the mobile network provider and user or service provider can more freely install and/or store user's authentication information on mobile device. The secret information can be in different formats depending on the type of services. For example, the user can use certificate that is stored on the mobile phone for authentication or install a specific application that contain user's private information and generate authentication token based on this information. The problem with this approach is that private information is stored on the mobile phone, so if the user changes mobile phone he/she has to acquire the same private information again.

SMS message is an example of authentication of the user based on private information that is received through mobile service operation. The most common scenario is that One Time Password (OTP) is delivered to user during authentication process, which afterwards must be inputted in the log in screen in the original application. Also other scenarios are developed. For example, when user receives a SMS message with the OTP he/she can just reply to the SMS message on the mobile phone. In this approach user is not required to retype OTP, but utilize the telephone network for the second factor of authentication Even thought this approach provides great usability to regular users (there is no need to use complicated application and functionalities of the mobile, but just SMS service that is well known to everybody), there are great trade-offs that this approach introduce. First, there are problems with latency of the SMS services especially during peak SMS usage as holidays. Another one is that text is transferred without any encryption and is visible to service provider. Also, a service provider has the right to store SMS messages on their side (for example when user is not accessible, so the message can be forwarded later on). Finally, there are also serious security vulnerabilities that this kind of authentication introduces e.g. man- in-the-middle attack.

Security level

Security level that is provided by using only this method is not so high. If an attacker steals the user's token or mobile device, he or she may gain full access to the user's private information and services. And today it is not so unlikely scenario that mobile phones are lost or stolen because of their small size and wide deployment in people everyday life. Mainly for this reason, this

approach for user authentication is usually used in combination with some other authentication method (most commonly with authentication based on something that user know e.g. password, PIN number). This approach is called two-factor authentication and is frequently used for user authentication for mobile services.

Usability issue

Usability of this authentication approach can vary greatly depending on the type of token used. For example, if authentication token is well chosen and the user is always in possession of token (for example if the token is the mobile phone), the whole authentication process can be very simple and easy for the user. But on the other hand we have examples where token is some stand-alone device which the user does not use very frequently and does not carry with her/him at all time. In these situations the user will often be unable to use the service, since he/she does not have the token present at that moment.

C. Something the user is

Ways to authenticate a user based on something he/she is are often based on scanning and analysis. These methods, referred to as biometrics, centers around authentication based on that person's unique traits. Traits can be physical, such as fingerprints or behavior, such as walking patterns or typing patterns [13] [17] [23].

Biometric authentication methods have been developed to counter the possibility that unauthorized persons may gain access when traditional security methods like security pass cards or passwords are used. In the article Making Palm Print Matching Mobile we can read that “the most critical flaw of these systems is that since they do not use any inherent characteristics or attributes of the individual user, they are unable to differentiate between an authorized personnel and an impostor who have fraudulently come to possess the token or knowledge (such as stolen credit card or lost password)." For this reason, various biometric methods have been developed in order to discern legitimate users. These methods include fingerprint-based systems and iris, retina, face, palm print, voice, handwriting and DNA technologies.

Stationary device approach

Several computer or keyboard models come equipped with finger-print-readers. They offer an alternative to authenticate the user of the machine in addition to traditional passwords. There are also some solutions that require the user to swipe their finger in order to get access to an area or

similar. In these cases the readers are attached to or close to doors.

Mobile device approach

In addition to desktop computers, many laptop models ship with fingerprint scanners that can be used for user authentication. With mobile phones, a few models are available with fingerprint scanners.

There have been and is ongoing research in this area, and as the technology improves, biometric scanners on mobile devices might be more widespread than what it is today. Some experiments, such as have been able to authenticate users based on palm print scanning using a mobile camera. Also ongoing research is conducted on authentication of users by scanning their wrist veins and recognizing their handwritten signature.

Security level

Some readers are easy to fool; requiring only a glove with an attached fingerprint according to Velum and Flesland some scanners may also accept cut-off fingers. Other scanners are more thorough and will not fall for simple tricks as this.

In addition, biometric solutions may pose a threat to the user itself. Imagine if unauthorized persons wanting access become aware that the only thing the user needs in order to gain access is to swipe one of his or her fingers. The user now runs the risk of having one of his fingers removed in order for the unauthorized persons to be able to gain access.

Until now there are also known attacks on fingerprint readers, using different materials to simulate finger (e.g. gummy bears). Biometrics might be best suited for additional security, or as a second factor in an authentication process, rather than being used on its own.

Usability issue

The use of biometrics can be quick and effective. Since it is based on something the user is, it is virtually impossible to lose or forget like tokens or passwords. After all, the user will always have his or her finger available for scanning. However, disabled people might not be able to utilize all biometric solutions. For instance a user in a wheelchair might not be able to utilize solutions based on walk patterns or a person with a broken arm will have trouble with maintaining the typing pattern he or she would have with both hands available. Some people might value their privacy more than the ability to use a convenient authentication method such as fingerprint scanning. Since

this is unique information that might be tied to a single person, their concerns may be justified. For a given solution, which information and how detailed as well as who might have access to this information might affect how a user reacts to such solutions. For one, it might be limited who really needs to store biometric information, like when entering schools Disneyland or even gyms. Another concern is if their information is somehow compromised, the users will not be able to change their fingerprint, like they would their password.

2.2.13. Types of security frameworks available and widely applied on M-Banking application and service are:

A. User name and PIN Security

It is something the user knows is often associated with any characters like a name, number. PINs should never be stored or processed in the clear anywhere in a system. Hash values of PINs should be encrypted to guard against brute-force attacks. Through PIN user is authenticated to the mobile network and he/she is protected from lost and theft. [17] [24]

There are numerous of attacks that can jeopardize user confidentiality and security. Some of the attacks are brute force attacks where attackers try to log into the service with every possible password until he/she succeed. Additionally, more threats can emerge if original password that is provided by use during registration is stored in an inappropriate manner.

One major problem with password and security is user factor. In most cases user is required to choose password that he/she will use on the system and remember it. PIN that is chosen can greatly influence security of the user, and because of that it is very important for user to choose strong password.

B. One Time Password (OTP)

OTP is a Random 6 digit number that changes every time, whenever user logs on the system and new password is generated and sent to the user on his mobile phone. OTP are utilized as an additional factor in multi-factor authorization/authentication applications. They are only valid for exactly one authorization or authentication request. The method of generating OTP whenever the user initiates a M-Banking transaction: - first step is the user enters his/her user name and password and allowed to login onto his webpage of his personal account, if the user authentication is valid. The user then initiates a transaction and the bank server respond back with OTP to his/her

mobile. This is the second level of authentication done to avoid password thefts. The user then authenticates with the OTP himself. The OTP is checked at the server and the transaction proceeds if valid [17] [24].

The OTP id valid only time every next time user logs in he needs to provide a new OTP that the user would have received at that particular moment of time. Threats to OTP are: wireless interception- the GSM technology is insecure due to several vulnerabilities such as a lack of mutual authentication and weave encryption algorithms. Mobile phone Trojans- malware and especially Trojans that are designed to intercept SMS messages contains OTPs.

C. Biometric Authentication

Biometrics is the science and technology of measuring and analyzing human body characteristics such as fingerprints, retina venial patterns, irises, voice patterns, facial patterns, and hand/finger measurements for authentication or identification purpose. Biometric identify people by measuring some aspect of individual anatomy or physiology (hand geometry of finger, voice, face). A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquiring data, and comparing this feature set against the template set in the database [17] [24].

The main benefits of Biometrics technology are to provide a better security and to facilitate the authentication process for a user. It is usually difficult to copy the biometric characteristics of an individual than most of other authentication methods such as passwords.

Biometric Modality

Each biometric information that can discriminate individuals is considered as a biometric modality.

The Biometric modalities are:

- Universality: all individuals must be characterized by this information
- Uniqueness: this information must be dissimilar as possible for two different individuals
- Collectability: it can be measured in an easy manner
- Acceptability: it concerns the possibility of a real use by users.

Table-2.1. Comparison of biometric modality [17]

Biometrics	U	N	P	C	A
DNA	Yes	Yes	Yes	Poor	Poor
Gait	Yes	No	Poor	Yes	Yes
Key stroke dynamics	Yes	Yes	Poor	Yes	Yes
Voice	Yes	Yes	Poor	Yes	Yes
IRIS	Yes	Yes	Yes	Yes	Poor
Face	Yes	No	Poor	Yes	Yes
Hand Gesture	Yes	No	Yes	Yes	Yes
Finger Print	Yes	Yes	Yes	Yes	Fair

U= universality, N= uniqueness, P= permanency, C= collectability, and A=acceptability

The biometric authentication process is divided into three main functionalities:

1. Enrolment: It constitutes the initial process of collecting biometric data samples from a person and subsequently creates a reference template representing a user's identity to be for later comparison.
2. Verification: It provides a matching score between the biometric samples provided by the user and his/her template. The matching score is defined between 0% and 100% (100% is quite impossible to be reached.
3. Identification: It consists of determining the identity of an unknown individual from a database of individuals. In this case, the system can then either attribute the identity corresponding to the most similar profile found in the database to the unknown individual or reject the individual.

Architecture of biometric system

The generic architecture of a biometric system consists of five main modules:

1. Capture module: It consists of capturing the biometric real data in order to extract a numerical representation. This representation is then used for enrollment, verification or identification.

2. Signal processing module: It allows the reduction of the extracted numerical representation in order to facilitate the processing time during the verification and identification phases.
3. Storage module: It is used to store biometric individuals' temples.
4. Matching Module: It is used to compare the extracted biometric raw data to one or more previously stored biometric templates. The module determines the degree of similarity between two biometric vectors.
5. Decision Module: It is used to determine if the returned index of similarity is sufficient to determine the identity of an individual.

2.3. Banking Applications in Ethiopia

2.3.1. Core Banking

A core banking system is the back-end data processing application for processing all transactions that have occurred during the day and posting updated data on account balances to the mainframe. Core systems typically include deposit account and CD account processing, loan and credit processing, interfaces to the general ledger and reporting tools.

All Banks in Ethiopian currently applied Core banking system to provide their services to the customer. Most of them applied T- 24 and Flexcube which are installed by Temenos AG and Oracle companies respectively.

TEMENOS T24

TEMENOS T24 is the most technically advanced banking system available today. It combines the most comprehensive and flexible business functionalities with the most advanced and scalable architecture. This gives it unprecedented power to meet the challenges of today and the opportunities of tomorrow. This application has a total of 37 modules and interfaces including Retail, Trade Services, Credit and Finance modules and Mobile Banking applications. It is a web based application where customers can access their account records, payment information, using personal laptop, mobile and so on. In this application, the company maintains financial and confidential information about its customers (Tin-number, account number, customer profile, and customer finical account, etc).

T24 runs on: three Open hardware, three Open database, three Open J2EE application server, three Open user interface through browser, HTML and XSLT, three Open connectivity through XML and Services, three Open C language code and three Open Java development environment

TEMENOS T24 can support:

• 1,000 transactions per second

• 10,000 signed-on users

• 100,000 signed-on Internet users

• 50,000,000 accounts

T24 allows you to improve application performance in a linear fashion by adding additional Capacity to an existing installation.

Oracle FLEXCUBE

Oracle Flexcube is one of the core banking system operated by some banks in Ethiopian. It is a compressive and integrated modular core banking system. Oracle flexcube can processing of large transaction volumes with high availability, Multiple delivery channel support, including branches, ATMs, point-of sale terminals, call centers, mobile devices, and internet banking. It is An XML Web based user interface with context-sensitive help, Security management covering application and role-based access, online validations and automated exception processing, Centralized, decentralized, and combination deployments. It has a capacity of ease of integration with existing systems using flexible Java Platform, Enterprise Edition technology. And Operational risk management controls, including limits, collateral.

2.4. Related Works

This section presents a review of some selected related works in Mobile Banking security frameworks for the banking industry. We will try to analyze and identify gaps that exist in previous works. Finally, we summarize the works reviewed.

Dr.D.S.Rao, GurleenKour and DivyaJyoti [8]: The title of the work is **One Time Password Security through Cryptography for Mobile Banking**. The objective of the work is to build a software application model for performing high security mobile banking services.

The major contribution of the work is the concept of One Time Password, which is every time a new password is generated and sent to the user on his mobile phone. The OTP is a random of 6 digits number that changes every time, whenever user logs on to the system and perform transaction. The limitation of the work is that, whenever the user initiate the service firstly he/she enters the username and the user redirected to another screen which prompted to enter the One Time Password that has been delivered on to the users registered mobile number at that particular moment of time. There are drawbacks to this approach. First, it pushes extra costs onto some end users, particularly in North America, where customers must pay for the messages they receive. Second, it is subject to network coverage, network latency and SMS delivery issues, which creates uncertainty over whether SMSs will be delivered quickly, or at all. Third, it doesn't address the Man-in-the-Middle fraud problem.

Mohammed Billa [21]: The title of the proposed work is **Security Issues in Mobile Banking**. The objective of the work to identify security risk in Mobile Banking and to provide an authentication method for mobile banking transaction by using biometric mechanism.

The major contribution of the proposed biometric mechanism is a finger-print scanning device which can identify the customer's finger print thus enabling the customer to access mobile banking services. The limitation of the work is that, it is applied only on those mobile devices which have finger print scanner.

J. Saranya 1, S. Thirumal 2 [33]: Thetitle of the proposed work is **Framework for secure mobile Banking Application using Elliptic Curve Cryptography and Image Steganography.**In this proposed solution, Elliptic curve cryptography is used which provides high-level security. On the other hand, to improve the security of data send from bank server to client, The overview of the proposed system is described in the image based Steganography is used. steganography is hiding message within something else in such away so that someone who doesn't know it is there will have trouble finding it .The limitation here is Huge file size, so someone can suspect about it. If this technique is gone in the wrong hands like hackers, terrorist, criminals then this can be very much dangerous.

The review of the existing literature showed that the security of mobile banking has been widely researched in the developed and emerging economies; however, we didn't get any research concerning the security of mobile banking technology in both bank and customer sides, for the developing Ethiopian economy. This research is therefore believed to fill this gap.

2.5. Gap Analysis

One of the major problems for the adoption of M-Banking is security issues from the customer side. It is to be recalled that M-Banking applications are added on the existing Banking applications. As the financial business has become more risky Banks core banking applications has to be equipped with better security platforms. This makes the Bank side highly secured. As mentioned before the M-Banking application two sides' one from the client side and the other end is the Bank side (due attention is given for the threat from the server side); it's to recalled that M-Banking operated via mobile device which is subjected to theft and other activities by potential attackers.

Accordingly, based on these facts we can say that previous works on security framework doesn't cover the overall security issues particularly from the client side. And as per our country security context more concern is given from the bank side. The existing security framework applied on M-Banking is single factor authentication, today single factor authentication, e.g. Passwords, is no longer considered secure in the Internet and banking world because Easy-to-guess passwords, such as names and ages, are easily discovered by automated password-collecting programs. Due to this fact and all which we investigated in our study. The current security framework is not protecting the security vulnerability from the client side. Therefore, our research addresses this gap by enhancing Multi Factor authentication by considering banking business security requirements and customer acceptance capacity.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1. Overview

This chapter discusses the processes and techniques used in carrying out the study. It also gives a description of the respondents including information on the study population, the number of respondents and how they were selected. It also provides an outline of research design and the instruments for data collection.

3.2. Research Design

A research design is a frame work or blueprint for conducting a research. It details all the necessary information needed to structure and solve the research problems. Even though a broad approach to the problem has already been developed, the research designs specify the details. The research design is the foundation on which the research is built. The information needed in the research was to assess and analyze customer satisfaction on service quality and customers concern (if any) on the security of the technology. The research design is the overall map for concerning the theoretical research problem to relevant and practicable empirical research which means it provides a plan or a framework for data collection and analysis. The rational, therefore, in this research is to explore and give explanation to the research questions posed.

We used survey method to understand the main barriers of customers in using the M-Banking technologies and propose adequate solution methods to overcome the problems. This method was used because it provides desired data. The questionnaire related to service quality elements and security concerns, among others.

Below is a conceptual model indicating the research process that is consists of a number of consecutive and related activities.

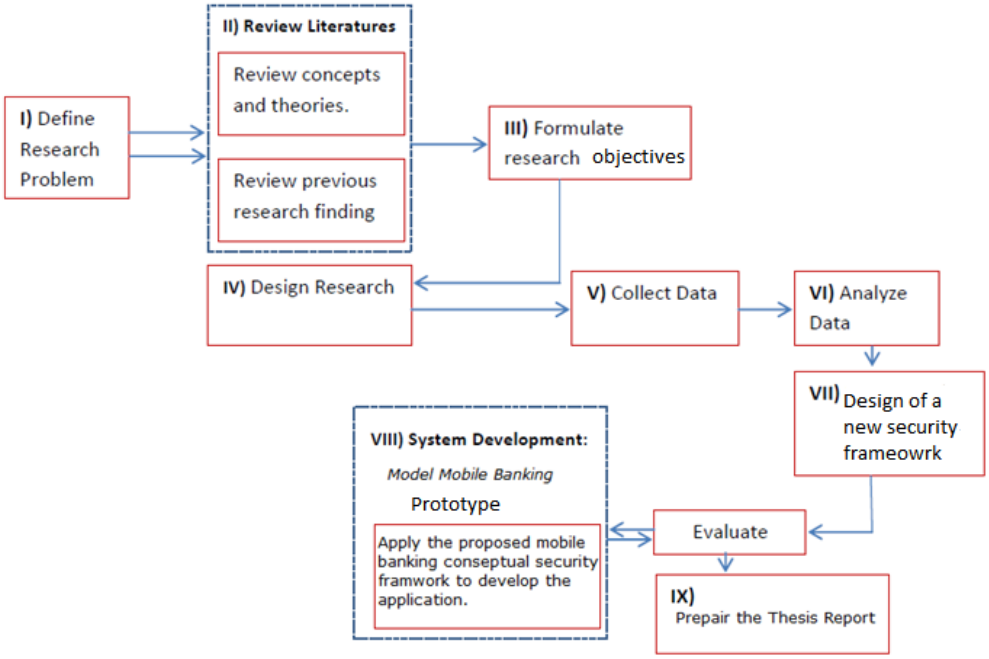


Fig 3.1 Research process flowchart [21].

3.3. Data Collection and Analysis Techniques

An analysis of existing researches which is relevant to the research topic, showing how it relates to the investigation is made so that to explain and justifies how the research investigation may help answer the questions or gaps in the area of research.

For collecting data to understand Mobile Banking Security framework at the mentioned Banks as a sample, the primary data consist of qualitative data that is obtained through interviews and questioner. The summarization of the interview and questioner result shed light onto the important and comprehensive data collected which directly tackle the subject being researched in this paper.

Secondary data source like books, reports, journal and conference articles and white paper from websites of reliable authors and organizations have been used to get information about Mobile Banking security framework and the security majors for banking industry.

3.4. Population and Sample

The population for the study consisted of customers of the CBE bank who transact in East Addis Ababa District Branches, professionals from CBE and two private banks called Nib international bank and Bank of Abyssinia, and experts from private ICT Company called BeabIcT Solutions - BITS. The sample for the study was made up of 420CBE customers, 20 selected professionals from CBE, 15 selected professionals from NIB, 20 selected professionals from bank of Abyssinia and 5 selected ICT experts from BeabIcT Solutions - BITS. The questionnaires were distributed to individual customers and the professionals to get a good response rate. The simple random sampling (SRS) method was used to select 420 CBE customers within the individual segment of customers from the forty branches located in East Addis Ababa District. From the 420 sample CBE customers, 370 were responded correctly, that is the overall response rate of the CBE customers achieved in the study was 88.1%. On the other hand, from the 60 professionals, 58 were responded correctly, that is the overall response rate of the professionals achieved in the study was 96.7%. Hence from all the distributed questionnaires, the response of 370 from CBE customers and 58 professionals were used in the research.

Custom insight software(http://www.custominsight.com/articles/randomsample-calculator.asp) was used to select sample size with 5% tolerable error level, with 90% of confidence level requires 272 samples but the sample was taken more than that i.e. 370. The questionnaire was distributed randomly to customers'. According to the banks report as of June 30, 2015 the number of accounts in the four district of Addis Ababa reached 1.6 million customers of which 534,000 in north Addis Ababa District, 351,000 in West Addis Ababa District 414,000 in South Addis Ababa District and 285,000 in East Addis Ababa District. 30 Branches under north Addis Ababa district retains 300,000 customers of the district. Sample sizes of 370 respondents were selected from these 30 branches located in East Addis Ababa city were selected due to cost and time constraints. The 370 respondents were selected randomly to assess the level of customers' satisfaction on M-Banking service quality and their security concerns.

3.5. Summary of Responses from the questions

Table 3.1 below shows the summary of the customer's responses in the selected questions from the questioner, relating to the M-Banking technology use and security concerns.

Table 3.1 Summary of customer's responses

No.	Question	strongly agree	agree	uncertain/ not applicable	disagree	strongly disagree
1.	I'm concerned about the security of mobile banking	72%	13%	9%	4%	2%
2.	My banking needs are being met without mobile banking	8%	12%	2%	25%	53%
3.	I don't see any reason to use mobile banking	20%	29%	10%	22%	19%
4.	The mobile phone screen is too small	29%	25%	22%	15%	9%
5.	I don't have a Smartphone	9%	12%	29%	28%	22%
6.	My bank charges a fee for using mobile banking	19%	21%	30%	22%	18%
7.	I don't do the banking in my household	25%	10%	14%	21%	30%
8.	I don't trust the technology	35%	22%	13%	18%	12%
9.	It's too difficult to use mobile banking	10%	12%	32%	29%	17%
10	My personal information will not be protected, if I use mobile banking	27%	25%	34%	8%	6%

Table 3.2 Below shows the summary of the professionals from the selected banks and experts from BeabIcT Solutions – BITS, responses in the selected questions relating to the M-Banking technology use and security concerns.

Table 3.2 Summary of the professionals and experts

No.	Question	strongly agree	agree	uncertain/ not applicable	disagree	strongly disagree
1.	I'm concerned about the security of mobile banking	73%	14%	7%	6%	-
2.	Ethiopian customer banking needs are being met without mobile banking	-	2%	9%	17%	72%
3.	A new security frame work is needed for mobile banking technologies in Ethiopia	79%	15%	6%	-	-
4.	Mobile banking adoption doesn't consider the social engineering of the customers	45%	21%	12%	15%	7%
5.	All applications must include local languages	29%	9%	11%	21%	25%
6.	Before adopting the technology, we need to do researches.	49%	25%	10%	7%	9%
7.	The security of the technology depends on the trustiness of individuals in the banks and ISP center.	47%	19%	22%	8%	4%

As shown in the above tables more than 85% of respondents cited their main reason for not using mobile banking was "I'm concerned about the security of mobile banking". In the same study, respondents were asked to rate their concerns on the security of mobile banking for protecting their personal information and 52% rated it as somewhat unsafe and very unsafe, while 34% were not sure of the security. These statistics represent a significant barrier to the use of mobile banking products and services in Ethiopia.

When you analyze the security risks of the mobile space, many of these feelings are not necessarily irrational. The lack of maturity of the mobile banking space brings many risks in the areas of new technologies, new inexperienced entrants in the ecosystem and a complex supply chain with risks in secure integration of the complex ecosystem. Many of these new entrants are innovative and dynamic with minimal experience or attention to security as a discipline. These

risks are most evident in the mobile application development and mobile hosting areas. New privacy risks are brought to light with personal data collected by the applications and information about the customer's physical location. Finally, customers are largely uneducated or have a high risk tolerance and unfortunately may opt into services that put their security and privacy in jeopardy

In-addition to the common mobile security issues occurred globally, based on the interview; we investigated some additional key risks which amplify the common risks. These include:

- The PIN or password to use the mobile banking applications are not encrypted with other characters and can easily be screen out by hackers around you.
- All SMS messages of transactions using mobile banking are not encrypted, so anyone who gets access to the mobile can easily get the text messages. In addition, the storage of copies of SMS messages at the SMS center server hosted by the mobile network service provider also provides a point of vulnerability to the SMS banking service. Since the message is in plaintext then any corrupted personnel who have access to the service providers SMS center server can easily view sensitive details.
- The strength of the PIN given by the banks is not adequate, and these may be easily identified by third person.
- Once you are authenticated to the application using the PIN, there is no any other mechanism to control sensitive transactions (such as check account, transfer money, and change PIN) of the application. This authentication method is not adequate, because simply hackers may easily get the PIN of a client using non-complex mechanisms such as security camera configuration or multiple mirror configurations of buildings where a client is predicted to open the application in.
- In the survey, respondents were asked to select how they recall their PIN and 57% save their PIN with other contacts on the same phone.

These additional security risks of mobile banking may led to financial and privacy violence's of individuals.

As per the review of the literature and the responses of the customers, professionals and experts we forced to propose a security framework for mobile banking key authentication and message exchange protocols. The proposed security framework for the Mobile Banking Key Authentication and Message Exchange protocols is described in the next chapter.

CHAPTER FOUR

THE PROPOSED CONCEPTUAL SECURITY FRAMEWORK

4.1. Overview

We have discussed on the security risks associated with mobile devices and have seen the main challenges of using the mobile banking applications globally. In the previous chapter, we have seen the summary of the main security issues of the existing mobile banking applications in Ethiopia and the responses of the selected sample on the distributed questioner. According to the responses and the investigated additional risks in mobile banking applications of Ethiopia, we find that security in the customer's side needs immediate action. According to [26] the three assets of mobile devices are device, application and private information. In the context of this thesis, these assets will be applied to the customer side of mobile banking application. The bank side (e.g. bank servers) and the network assets (e.g. telecom provider) are not the scope of this research.

This chapter presents the proposed security framework for mobile banking key authentication and message exchange protocols. Key management is the main concern in protecting to the entry point of an application and private information's loaded on a device. For the sale of performance of the customer's devices in running the mobile banking application, we use symmetric key cryptosystem in our proposed protocols because the SMS application can't perform heavy encryption operations.

4.2. Key Generation

The proposed protocols use a strong random key generator algorithm to create the activation key, PIN and list of one time passwords. This key generator must be maintained and owned by the banks. The list of the generated keys will be written to a file, print securely and sent the printed one to the client using a secure communication media upon request. In the event of check balance, transfer money and change PIN protocols the client encrypts the request with one of the randomly generated password. The reply from the bank is encrypted using a key derived from the concatenation of the clients PIN and account number. When the reply message is received by the client he or she needs to enter both the PIN and account number in

order to access the massage content. The advantage here is that there is no need to store the generated one time password after using to check balance or transfer money or change PIN.

4.3. Proposed Key Management

- A registered mobile banking user of the bank is required to have a bank account, PIN and activation key where only the customer and bank database should know these keys.
- The user during at time of registration receives the activation key and PIN in a secure manner from the bank. The bank generates these keys in encrypted form, prints by decrypting the generated once in a secure way and uses a secure delivery channel to send it to the client, where only the bank database should know.
- The user receive, list of one time passwords after the activation process is accomplished by changing a PIN of his own choice.
- The user can receive list of one time passwords whenever he or she finishes the list. In addition, the bank can discard and generate new list of one time passwords on the request of the user.

4.4. Application of the Proposed Security Framework

This section presents the proposed security framework for message exchange and transaction protocols. We separate protocols for the activation process, change PIN, check balance and money transfer transactions. Once a user is authenticated to interact with the mobile banking page using his or her activation key and PIN, he or she needs to change the PIN to use the services of the mobile banking (change PIN, Check Balance or Transfer Money). After changing a PIN of customer's choice, the activation key is discarded from the database of the bank and the client needs to use his or her PIN to use the application again. The client requires to select one from the given one time passwords and if succeed with that, the password will be discarded from the database of the bank and can't be used again.

4.4.1. Activation Process

Level 1: Registration Process

The mobile banking services are provided only to the customers who have specifically opted for the same and registered as described above.

Level 2: Activation Process and PIN Change

Customer has to activate the application using an activation key given by the bank at the time of registration and is requested to create a 4-digit numeric PIN of his choice at the time of activation. The activation key is discarded from the banks database after changing the PIN.

Level 3: User-Generated PIN

Customer can also change the 4-digit numeric PIN when required. This acts as a verification mechanism to enter the application. The application gets locked in case of three incorrect PIN entries.

Level 4: Storage encryption

All data that is stored on the phone/client is encrypted using the PIN and client account identification encryption standards thereby making it secure.

Level 5: Communication encryption

The data exchanged between client and server is encrypted using PIN, account identifications and one-time passwords.

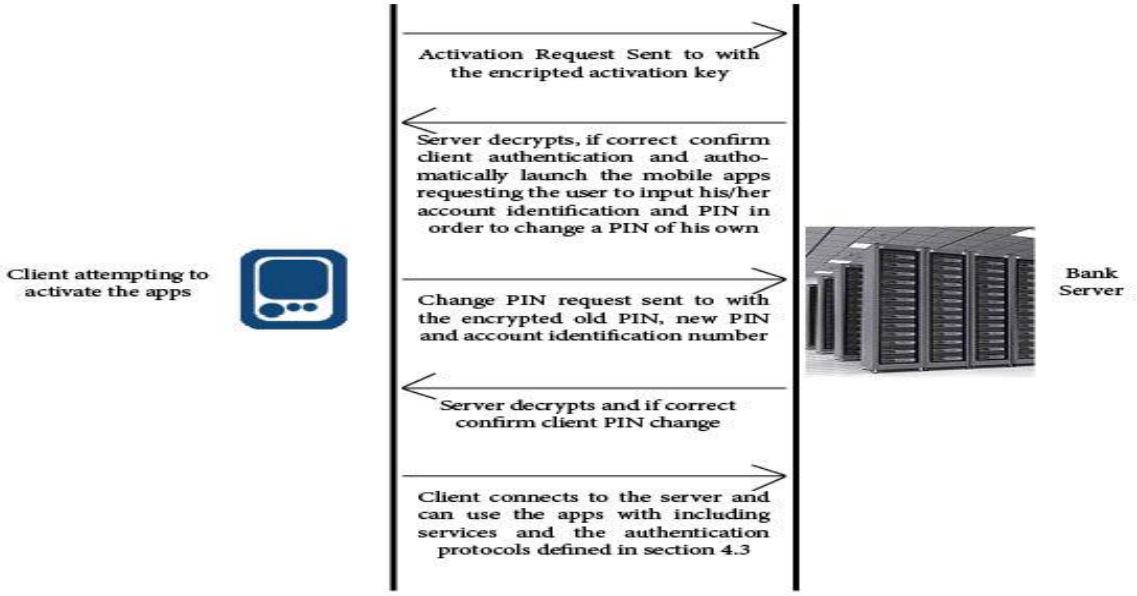


Fig 4.1.The activation process

4.4.2. PIN Change Protocol

In the PIN change protocol a single encrypted message is sent to the bank server by the client. The message δ is encrypted using the one time password, transaction type, client identification, old PIN and new PIN. The message abstraction is generated by a hash function $\hbar_{cb}$ and sent to the banks server. A hash function $\hbar_{bc}$ display a verification message or error message as a result of the generated message abstraction. The protocol is presented as follows.

PC_{cb} : C → B : $\hbar_{cb}[\delta]$

PC_{bc} : B → C : $\hbar_{bc}$ [$\hbar_{cb}[\delta]$] = [<Verification>] or [<Error Message>]

Where

- δ = [CAI | TT | OPW | OPIN | NPIN]
- TT=0 is a number specifying the selected transaction, which is PIN change
- CAI is the client account identification of the user
- OPW denotes the one time password
- OPIN denotes the old personal identification number of the client, which is in use.
- NPIN denotes the new personal identification number of the client, which the client want to change to.
- $\hbar_{cb}$ denotes a hash function encryption with the client account identification, transaction type, one-time password, old PIN and new PIN.
- $\hbar_{bc}$ displays a simple text box which is a reply from the bank confirming the PIN change and automatically sign out from the application. In case of any error in the input data or technical error from the bank database connection, $\hbar_{bc}$ displays an error message.

Once a password has been used it will be considered as expired and the system will not recognize it if it is reused.

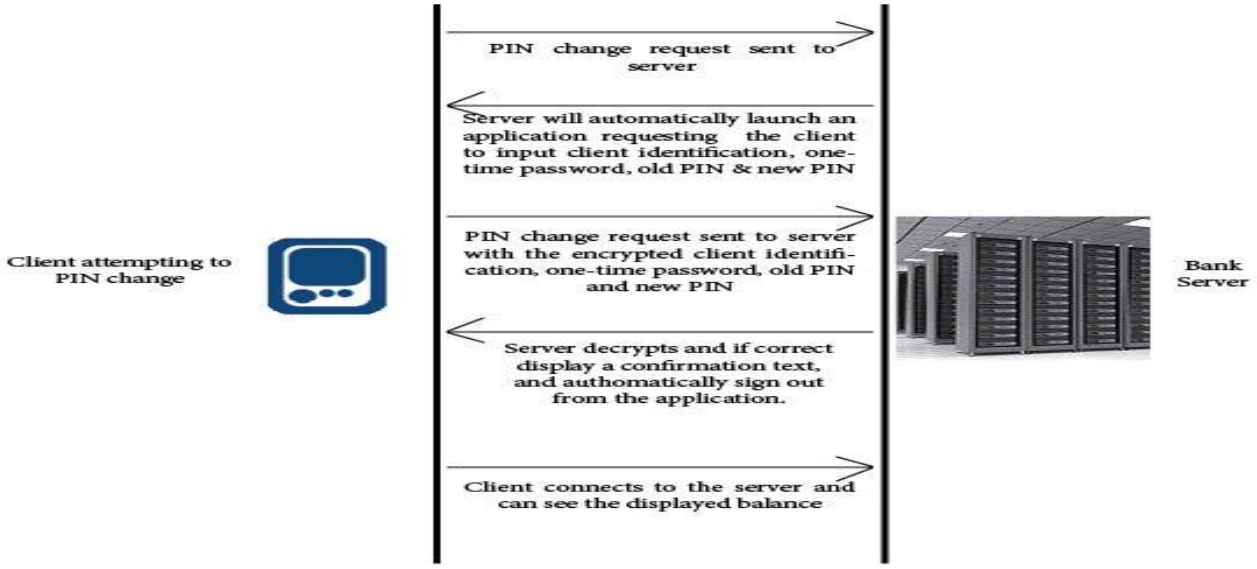


Fig 4.2. The PIN change protocol

4.4.3. Check Balance Protocol

In the check balance protocol a single encrypted messageμ is as well sent to the bank server by the client. The message μ is encrypted using the one time password, transaction type, client identification and PIN. The message abstraction is generated by a hash function $Ħ_{cb}$ and sent to the banks server. A hash function $Ħ_{bc}$ display a simple message containing information of balance or displays error message as a result of the generated message abstraction. Additionally the hash function $Ħ_{bc}$ generates an encrypted SMS message using the current PIN and client identification in case the client needs to read any time without opening the application.

The protocol is presented as follows.

CB_{cb} : C⟶B : $Ħ_{cb}[μ]$

CB_{bc} :B⟶C : $Ħ_{bc}$ [$Ħ_{cb}[μ]$] = [<balance information>] or [<Error Message>]

Where

- μ = [CAI | TT| OPW| PIN]
- TT=1 is a number specifying the selected transaction, which is check balance
- CAI is the client account identification of the user
- OPW denotes the one time password
- PIN denotes the personal identification number of the client

- H_{cb} denotes a hash function, encryption with the client account identification, transaction type, one-time password and PIN.
- H_{bc} denotes a hash function display a simple message containing the clients balance information and reply encrypted SMS message from the bank using concatenation of the user account identification& PIN which will automatically launch a display requesting the client to input client identification & PIN. In case of any error in the input data or technical error from the bank database connection, H_{bc} displays a text which is a reply from the bank denoting the error message.

Once a password has been used it will be considered as expired and the system will not recognize it if it is reused. The client will be requested to input his/her account identification and current PIN in order to access the message any time.

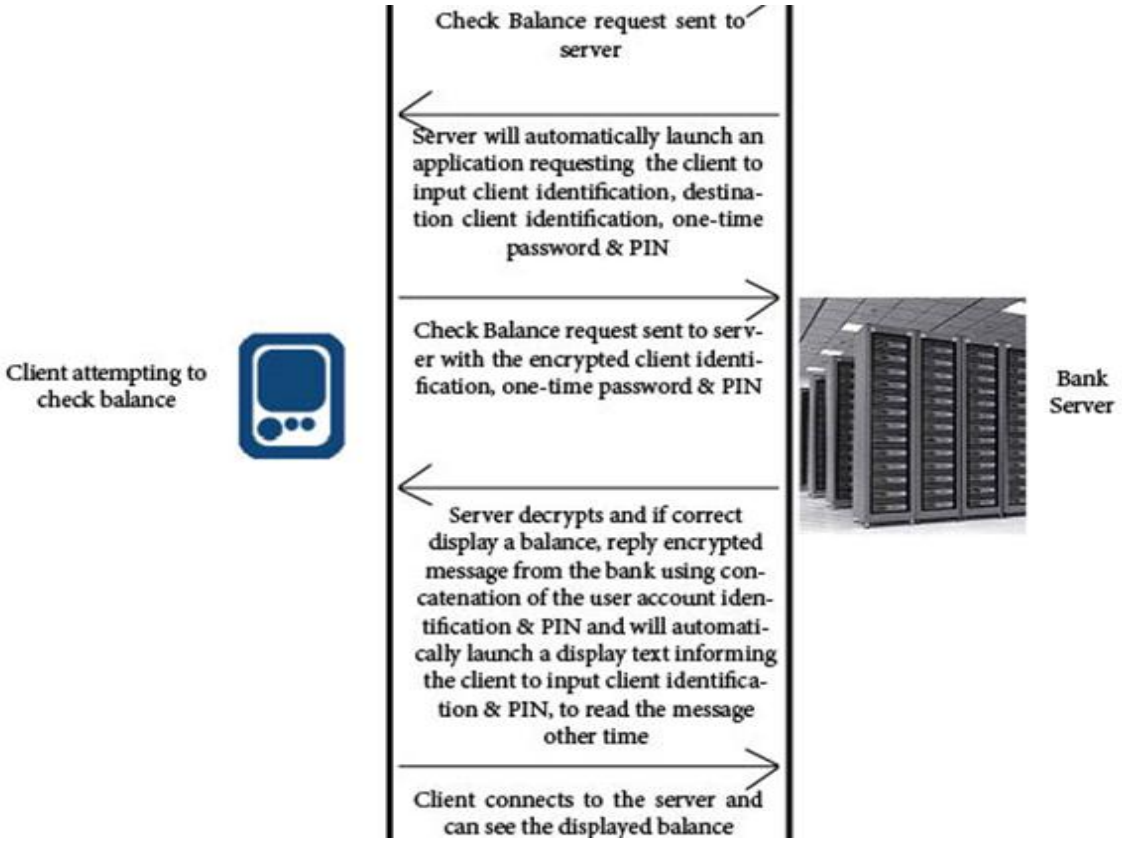


Fig 4.3. The check balance protocol

4.4.4. Money Transfer Protocol

In the check balance protocol a single encrypted messageα is as well sent to the bank server by the client. The message α is encrypted using the one time password, transaction type, client

identification, destination client account identification and PIN. The message abstraction is generated by a hash function H_{cb} and sent to the banks server. A hash function H_{bc} reply after 3 minutes. If the client doesn't take any action in canceling the transfer action, assuming the confirmation of the transaction by the client, the hash function will display a simple message confirming the balance transfer or displays error message as a result of the generated message abstraction. Additionally the hash function H_{bc} generates an encrypted SMS message using the current PIN and client identification in case the client needs to read the transfer any time without opening the application.

The protocol is presented as follows.

MT_{cb} : C⟶B : $H_{cb}[\alpha]$

MT_{bc} : B⟶C : H_{bc} [$H_{cb}[\alpha]$] = [<Verification>] or [<Error Message>] in plaintext.

Where

- α = [CAI | DAI | TT | Amount | OPW | PIN]
- TT=2 is a number specifying the selected transaction, which is balance transfer
- CAI is the client account identification of the user
- DAI is the destination account identification of the client to which the money will be transferred.
- Amount is the amount of money which will be transferred from CAI to DAI
- OPW denotes the one time password
- PIN denotes the personal identification number of the client
- H_{cb} denotes a hash function encryption with the client account identification, destination account identification, transaction type, one-time password and PIN.
- H_{bc} denotes a hash function reply after 3 minutes encrypted message from the bank using concatenation of the user account identification & PIN, and will launch a display requesting the client to input client identification & PIN, to read the message other time. In case of any error in the input data or technical error from the bank database connection, H_{bc} displays a text which is a reply from the bank denoting the error message.

Once a password has been used it will be considered as expired and the system will not recognize it if it is reused. If the authentication is successfully passed with all the input data,

the money transfer transaction will take place after 3 minutes and display a massage confirming the transfer, unless the client send an authenticated cancel message within 3 minutes or any technical error from the bank database. Additionally the hash function H_{bc} generates an encrypted SMS message using the current PIN and client identification in case the client needs to read the transfer any time without opening the application.

.

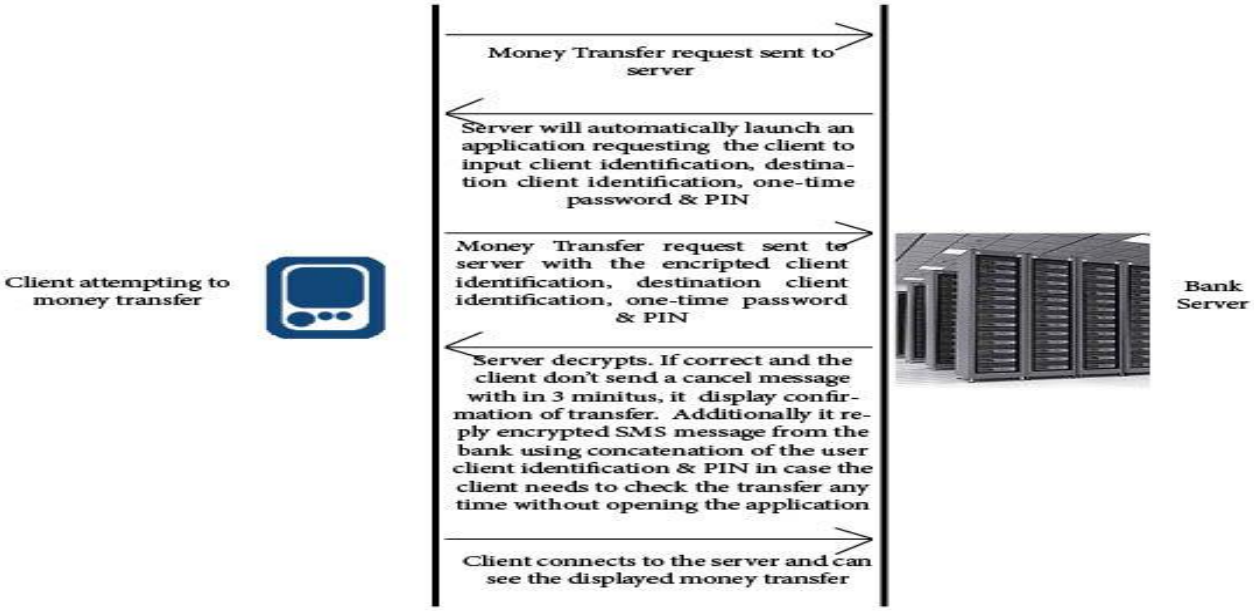


Fig 4.4. The transfer money protocol .

4.5. Security Measures of the Proposed Framework

This section describes the security considerations regarding integrity of personal information, Authentication, Repudiation and Confidentiality [31].

4.5.1. Integrity

The protocol employs a hashing algorithm to create a message digest of the message exchanged. The message digest is calculated both at the mobile phone application and at the bank server this is performed by integrity check algorithm incorporated with our proposed framework. The fields

that constitute the digest are discussed in the previous chapter. If the content is altered during transmission a mismatch digest will occur and the receiver will know that the message has been compromised.

4.5.2. Authentication

For authentication purposes the protocol includes the personal identification number (PIN) where only the customer and bank database should know this PIN. The client during time of registration receives the list of one time passwords in a secure manner from the bank. This can be done by the client physically collecting them from the bank or the bank uses a secure delivery channel to send it to the client. The client enters his banking details that include the account and PIN in the mobile application and are used for authentication at the bank server side.

4.5.3. Non Repudiation

In our protocols non-repudiation is ensured through the use of the PIN, one time password and account number that are known only to the client and the bank. If the message is successfully decrypted by the bank, then it indicates the corresponding client must have sent the message. The client cannot therefore deny having sent the message. We strongly assume here that the bank has concrete security policies on how it internally handles access to its client details like PIN in its database.

According to [15], banks have traditionally fought fraud from within and outside. In the case of insider fraud security audits and functional separation are notable methods used. However with increased complexity of banking systems banks now employ Hardware Security Modules (HSM's) that are used to protect PIN derivation keys from corrupt employees and physical attacks.

4.5.4. Confidentiality

This is achieved in check balance, money transfer, and PIN change and activation protocols by encrypting the message using a onetime password, PIN authentication and client account identification. It is assumed that only the client and bank have knowledge of these.

CHAPTER FIVE

EVALUATION OF THE PROPOSED CONCEPTUAL FRAMEWORK

This chapter considers a real world scenario to evaluate the proposed conceptual security framework by developing a model mobile banking application that incorporates major banking functionalities. Accordingly, the satisfaction of the users is serviced by presentation the research questionnaires once ageing. Below are details of the evaluation process:

5.1. A Prototype Implementation

- The console application is developed using Python programming language.
- Here we choose bcrypt and other cryptography libraries to use:
    - bcrypt is a password hashing function.
    - Cryptography includes both high level recipes and low level interfaces to common cryptographic algorithms such as symmetric ciphers, message digests, and key derivation functions.

5.2. Evaluation Input

- Twenty Experts and Thirty CBE customers who have actively participated on responding the initial research questioner were contacted once again to evaluate the proposed mobile banking security framework and fortunately, all were willing.
- A workstation, my computer, with the model mobile banking application installed was prepared for the customers to use it while doing the evaluation.
- The customer account registered in the model application holds a deposit of 12,500 birr and the tester were provided to perform whatever transaction he/she desire.
- At the end of the evaluation, testers were expected to respond the questioners as he/she have done on the initial phase of this research.

5.3. Sample Evaluation Scenario

Scenario 1: Performing Transaction Using Mobile Banking

- Tester A , a customer of CBE, performs the following transaction :
  - Log on to the system

```
Welcome to mobile banking system
Please enter pin number:
```

```
Please enter one time password:
Please enter new pin:
```

```
Pin chnaged sucessfully
```

  - Check his current balance

```
Welcome to mobile banking system
Please enter pin number:

        1.Check Balance
        2.Transfer Money
        3.Change Pin
        4.Exit/Quit

What would you like to do? 1
```

```
What would you like to do? 1
Please enter one time password:
```

```
Your balance is: 12500.0

        1.Check Balance
        2.Transfer Money
        3.Change Pin
        4.Exit/Quit

What would you like to do?
```

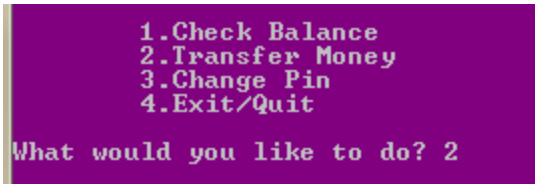
  - Transfer birr 2000 to account number 1002

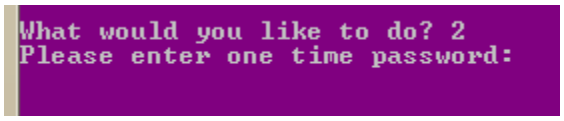
```
What would you like to do? 2
Please enter one time password:
```

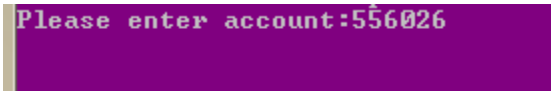
```
Please enter account:1002
```

```
Please enter the amount:2000
Your remaining balance is: 10500.0
```

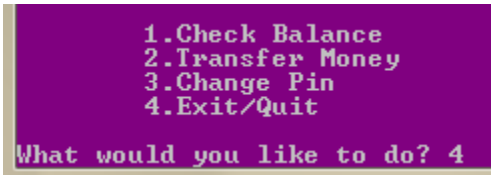
  - Again , He transfer birr 500 to account number 556026







- Finally, he logged out.



Scenario 2: Message Encryption

- The concept behind the message encryption process is that to mask any transactional information of a customer sent via a short text message to the customer so that no one except the customer has the capability of viewing the text information even though the customer mobile phone is not under his/her custody.
- The right customer will read the message sent from banks by entering his/her pin and account number.

Summery

- Every time a new tester (customer) login to the system for the first time, the system request to enter his/her pin number provided by the bank and also forced to enter a new pin number. The inputted pin and one time password is not visible for the end user in a masked or plain text, which make the proposed approach more secure.

- Every time the customer performs a transaction, he/she requested to input one time password; which is additional authentication technique proposed by this paper that was not been practiced before in Ethiopian mobile banking applications.

5.4. The Evaluation

- The testers respond to the questionnaires after evaluating the proposed mobile banking security framework using the model system .Their response is summarized below in short:

Table 6.1 Summary of customer and Expert response on the proposed mobile banking security framework

No.	Question	strongly agree	agree	uncertain/ not applicable	disagree	strongly disagree
1.	I'm concerned about the security of mobile banking	30%	5%	5%	10%	50%
2.	I don't trust the technology	10%	5%	10%	25%	50%
3.	A new security frame work is needed for mobile banking technologies in Ethiopia	90%	10%	-	-	-
4.	It's too difficult to use mobile banking	5%	7%	22%	56%	10%
5.	The security of the technology depends on the trustiness of individuals in the banks and ISP center.	47%	19%	22%	8%	4%
6.	My personal information will not be protected, if I use mobile banking	5%	10%	25%	30%	30%

5.5. Evaluation Result and Its Implication

- Customers concern about the security of mobile banking while using the model mobile banking application which is developed by the proposed conceptual security framework is found to be much less (reduced with 50 %) than the concern rate in using the current mobile banking application of Ethiopian banks.
- Customers concern about personal information protection is found to be much reduced with 60% that the concern rate in using the current mobile banking application.
- Finally, our evaluation fulfills the security considerations regarding integrity of personal information, Authentication, Repudiation and Confidentiality.

CHAPTER SIX

CONCLUSIONS AND RECOMMENDATIONS

In this chapter we give our conclusions and recommendations on the application of our proposed security framework for Mobile Banking Key Authentication and Message Exchange Protocols: in the case of Ethiopia. We present the challenges and opportunities of such systems and end the chapter with a conclusion of this work and highlighting future areas for further exploration.

6.1. Conclusions

The thesis reviewed the current state of mobile banking and SMS exchange services in Ethiopia and highlighted the technologies and security shortfalls of enabling systems utilizing ordinary plaintext SMS message communication. From the study of these systems and related ones we have come up with a an approach that will strengthen the mobile banking security and evaluate its rate of satisfaction and confidence by analyzing the response of customers and expertise for a questioners presented to evaluate the model mobile banking application developed as per the proposed conceptual security framework.

This paper articulates current mobile banking problems and discusses the need for strong security implementation on both server and client's sides for the Ethiopian banking industry. The general objective of this paper was to propose a generic Mobile Banking Security framework in the client's side, for the Ethiopian banking industry.

To achieve the objective, we selected the Ethiopian banking industry to understand the current Mobile Banking security of the client's side, by investigating the main concerns of customers for not using the service. We identify that their main concern was on the authentication keys of the application including the message exchange process. After gaining knowledge from the survey study, then put it in to the existing knowledge on the subject matter, which are identified from literature reviews. Finally, we come up with a new framework that helps the banking industry for exercising the security of mobile banking key authentication and message exchange. In summary we are optimistic our system can gain acceptance in society given the security benefits it offers.

6.2. Recommendations

The potential for SMS mobile banking services is particularly high in countries were Internet infrastructure hinders the access to electronic banking services. In Ethiopia Internet connectivity and bandwidth are low and the population is not urbanized and averagely poor hence making realization of internet banking services not viable in most parts of the country. We therefore note that for the foreseeable future given the high diffusion rate of mobile telephony in Ethiopia SMS banking is the most viable option for offering affordable remote banking transactions.

The success of SMS banking will mainly depend on the banking industry on how they perceive the usefulness of the system to enable them offer better services to their clients and help reduce in their operating costs. The potential of the general adoption of SMS banking is there given the fact that clients give a lot of attention to convenience and accessibility of personal accounts when choosing a banking service provider.

We recommend that customer side URL inspection tool should further be developed for its performance and compatibility and thorough testing should be done and also in the future the research should consider the usability issues. This depends on what constitutes an acceptable security level and on the trade-off between usability and security.

REFERENCES

[1]. Gavin Troy, "Mobile Banking Technology Options", Available at http://www.gsma.com/mobilefordevelopment/wpcontent/uploads/2012/06/finmark_mbt_aug_07.pdf (accessed on April, 2016)

[2]. Mahmood Shah and Steve Clarke, E-Banking Management, Issues, solutions & strategies, British Cataloguing, India, 2009, pp. 1-8,30-52,

[3]. Gardachew Worku, "Electronic-Banking in Ethiopia: practices, opportunities and Challenges", *Journal of internet Banking and commerce*, vol 15(2): pp 2-9, 2010

[4]. Aychiluhim Desisa and Tibebe Beshah, "Internet Banking Security Framework: The case of Ethiopian Banking Industry", *HiLCoE Journal of Computer Science and Technology, Vol. 2, No. 2, 2014*

[5]. Finmark Trust (2008, March), "Managing the Risk of Mobile Banking Technologies", Bankable Frontier Associates LLC, *pp 50-65 Available www.bankablefrontier.com, 2008*

[6]. Elad Barkan, Eli Biham and Nathan Keller, "Instant Cipher text-Only Cryptanalysis of GSM Encrypted Communication", CRYPTO, LNCS 2729, pp. 600 - 616, 2003

[7]. Jin Nie and Xianling Hu, "Mobile Banking Information Security and Protection Methods", International Conference on Computer Science and Software Engineering, pp. 587-590, 2008, Available at http://doi.ieeecomputersociety.org/10.1109/CSSE.2008.1422.pdf (accessed on March 2016)

[8]. Biryukov, Shamir and Wagner, "Real Time: Cryptanalysis of A5/1" on a PC Department of Computer Science, the Weizmann Institute, Rohovot Israel.

[9]. Kelvin Chikomo and Ming Ki Chong, "Security of Mobile Banking" Data Networks Architecture Group, University of Cape Town, South Africa,

[10]. Abunyang Emmanuel, "Mobile Banking in Developing Countries: Secure Framework for Delivery of SMS-banking Services", M.A. thesis, *Radboud University, Netherland, 2007.*

[11]. Klaus Vedder, "GSM: Security, Services, and the SIM", Springer Verlag, Berlin Heidelberg, LNCS 1528, pp. 224-240, 1998

[12]. Jorge Aguila, Jetzabel Serna, Manel Medina and Andreas Sfajianakis, "A professional view on E-Banking authentication challenges & recommendations", presented at the 9th International Conference, Information Assurance and Security, Tunisia, 2013

[13]. Gurmeet Singh Saini, (2014, March) "Mobile Banking in India, Issues and challenges", SaiOm Journal of Commerce and Management, Vol 1, issue 3, pp. 30-37, Available at http://www.saiompublications.com (accessed on March, 2016).

[14]. Bruce Schneier, "Attack Trees: Modeling security threats", Dr.Dobb's Journal, 1999

[15]. Agwu, Edward, "Generations X and Y Adoption of Internet and Internet Banking in Nigeria", International Journal of Online Marketing, vol 4, pp. 68-81, 2012

[16]. Aman Yehun, "Mobile Commerce" First from Dashen, 2016

[17]. Ross Corkery and Lynne Parkinson, "Interactive Voice Response" Behavior Research Methods, Instrument and Computer, vol 34(3) pp 342 – 353, 2002

[18]. Kenneth G. Paterson and Douglas Stebila: "One Time Password Security through Cryptography for Mobile Banking" Information Security Institute, Queensland University of Technology, Australia, 2009

[19]. John W. Muchow, "Core J2ME Technology and MIDP", the Sun Microsystems Press-Java Series, 2002

[20]. John Sherwood, Andrew Clark and David Lynas "Enterprise Security Architecture" *SABSA*, White. . Paper, 1995-2009 SABSA Limited.

[21]. Kelvin Chikomo and Ming Ki Chong, "Security of Mobile Banking" Data Networks Architecture Group, University of Cape Town, South Africa,

[22]. Mike Bond and Piotr Zielinski, "Decimalization table attacks for PIN Cracking" in proc. UCAM-CL-TR-ISSN, 2003, University of Cambridge http://www.cl.cam.ac.uk/

[23]. Naresh K. Malhora and David F. Briks, "Marketing Research, Business and Economics", 2007

[24]. NiinaMallat, Matti Rossi, and Virpi Kristiina Tuunainen, "Mobile Banking Services Communications" Communication of the ACM – New architecture for financial, vol 47 issues 5, pp 42-46, 2004

[25]. Tasneem G. Brutch and Paul C. Brutch, "Mutual Authentication, Confidentiality, and Key Management (MACKMAN) System for Mobile Computing and Wireless Communication", IEEE Annual Computer Security application conference, 1998 pp 35 – 73.

[26]. Vanessa Pegueros, "Security of Mobile Banking and Payments", GIAC (GSEC) Gold Certification, SANS Institute InfoSec Reading Room, 2012.

[27]. ETSI Secretariat, “Digital cellular telecommunications system (phase 2+)” France, European Telecommunication Standard Institute, ICS 33.020, July, 1999.

[28]. S. Bradner, “Wireless Application Environment” WAP Forum http://www.wapforum.org

[29]. William Stallings, “Network Security Essentials”, Pearson Education, Inc. Upper Saddle river, New Jersey USA, 2003

APPENDICES

Sample Mobile banking application Code using python

```
# Author Betelhem Belete
# Date June 2017

import getpass
import bcrypt
from cryptography.fernet import Fernet

# menu function
customers = [{'pin': '4444', 'account_no': '1001', 'firstname': 'Betty', 'lastname': 'Belete',
'gender': 'Female'},
        {'pin': '5555', 'account_no': '1002', 'firstname': 'Abebeb', 'lastname': 'Kebede',
'gender': 'Male'}]

passwords = [{'pin': '4444', 'account_no': '1001', 'pass':
b'$2b$12$4kO8SDoGoJ2B1.Mo9qv1DepG/IO7Dm2orXAAX0YP9PON6jTQ49Sbq',
'type': 'cb', 'status': 'Active'},
        {'pin': '4444', 'account_no': '1001', 'pass':
b'$2b$12$4kO8SDoGoJ2B1.Mo9qv1DepG/IO7Dm2orXAAX0YP9PON6jTQ49Sbq','typ
e': 'mt', 'status': 'Active'},
        {'pin': '4444', 'account_no': '1001', 'pass':
b'$2b$12$4kO8SDoGoJ2B1.Mo9qv1DepG/IO7Dm2orXAAX0YP9PON6jTQ49Sbq','typ
e': 'cp', 'status': 'Active'},
        {'pin': '5555', 'account_no': '1002', 'pass':
b'$2b$12$4kO8SDoGoJ2B1.Mo9qv1DepG/IO7Dm2orXAAX0YP9PON6jTQ49Sbq','typ
e': 'cb', 'status': 'Active'},
        {'pin': '5555', 'account_no': '1002', 'pass':
b'$2b$12$4kO8SDoGoJ2B1.Mo9qv1DepG/IO7Dm2orXAAX0YP9PON6jTQ49Sbq','typ
e': 'mt', 'status': 'Active'},
```

```
        {'pin': '5555', 'account_no': '1002', 'pass':
b'$2b$12$4kO8SDoGoJ2B1.Mo9qv1DepG/IO7Dm2orXAAX0YP9PON6jTQ49Sbq',
'type': 'cp', 'status': 'Active'}]

balances = [{'pin': '4444', 'account_no': '1001', 'balance': 12500.00},
        {'pin': '5555', 'account_no': '1002', 'balance': 5200.00}]


def menu():

    print("Welcome to mobile banking system")

    ans1 = 1

    while ans1 <= 3:
        # getpass function recive pin number without printing it
        pin = getpass.getpass('Please enter pin number:')
        if not check_pin(pin):
            print('Invalid pin number')
            ans1 = ans1 + 1
            if ans1 == 4:
                return
        else:
            break

    pin = change_pin_first_time(pin)


    ans = True
    while ans:
        print ("""
```

```
        1.Check Balance
        2.Transfer Money
        3.Change Pin
        4.Exit/Quit
        """)
        ans = input("What would you like to do? ")
        if ans == "1":
            check_balance(pin)
        elif ans == "2":
            transfer_money(pin)
        elif ans == "3":
            change_pin(pin)
        elif ans == "4":
            print("\n Goodbye")
            return
        elif ans != "":
            print("\n Not Valid Choice Try again")


def check_balance(pin):

    passw = getpass.getpass('Please enter one time password:')

    # generate symmetric key for encrypting user password
    key = Fernet.generate_key()
    cipher_suite = Fernet(key)

    cipher_text = cipher_suite.encrypt(passw.encode('utf-8'))

    for pwd in passwords:
```

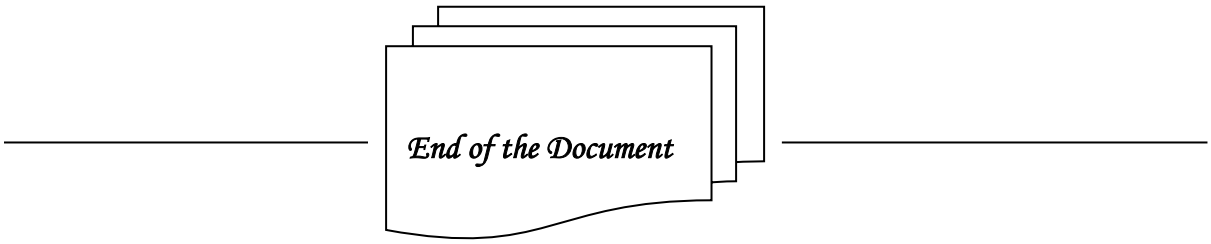
```
        if pwd['type'] == 'cb' and pwd['pin'] == pin and
bcrypt.checkpw(cipher_suite.decrypt(cipher_text), pwd['pass']) and  pwd['status'] ==
'Active':
            # change password status
            pwd['status'] = 'Closed'

            print('Your balance is:', get_balance(pin))
            return

    print("Invalid Password")


def change_pin(pin):

    passw = getpass.getpass('Please enter one time password:')

    # generate symmetric key for encrypting user password
    key = Fernet.generate_key()
    cipher_suite = Fernet(key)

    cipher_text = cipher_suite.encrypt(passw.encode('utf-8'))

    for pwd in passwords:
        if pwd['type'] == 'cp' and pwd['pin'] == pin and
bcrypt.checkpw(cipher_suite.decrypt(cipher_text), pwd['pass']) and  pwd['status'] ==
'Active':
            # change password status
            pwd['status'] = 'Closed'

            # change pin
            newpin = getpass.getpass('Please enter new pin:')
```

```
            # change pin in password list
            for pwd1 in passwords:
                if pwd1['pin'] == pin:
                    pwd1['pin'] = newpin

            # change pin in cutsomer list
            for customer in customers:
                if customer['pin'] == pin:
                    customer['pin'] = newpin

            # change pin in balance list
            for balance in balances:
                if balance['pin'] == pin:
                    balance['pin'] = newpin

            print("Pin chnaged sucessfully")

            return

    print("Invalid Password")

def change_pin_first_time(pin):

    for pwd in passwords:
        if pwd['type'] == 'cp' and pwd['pin'] == pin  and pwd['status'] == 'Active':
            # change password status
            # pwd['status'] = 'Closed'

            # change pin
            newpin = getpass.getpass('Please enter new pin:')
```

```
            # change pin in password list
            for pwd1 in passwords:
                if pwd1['pin'] == pin:
                    pwd1['pin'] = newpin

            # change pin in cutsomer list
            for customer in customers:
                if customer['pin'] == pin:
                    customer['pin'] = newpin

            # change pin in balance list
            for balance in balances:
                if balance['pin'] == pin:
                    balance['pin'] = newpin

            print("Pin chnaged sucessfully")

            return newpin

        print("Invalid Password")


def transfer_money(pin):

    passw = getpass.getpass('Please enter one time password:')

    # generate symmetric key for encrypting user password
    key = Fernet.generate_key()
    cipher_suite = Fernet(key)
```

```
    cipher_text = cipher_suite.encrypt(passw.encode('utf-8'))

    for pwd in passwords:
        if pwd['type'] == 'mt' and pwd['pin'] == pin and
bcrypt.checkpw(cipher_suite.decrypt(cipher_text), pwd['pass']) and pwd['status'] ==
'Active':
            # change password status
            # pwd['status'] = 'Closed'

            # enter account
            account = input('Please enter account:')
            amount = input('Please enter the amount:')

            for balance in balances:
                if balance['account_no'] == account:
                    for b1 in balances:
                        if b1['pin'] == pin:
                            if float(amount) > float(b1['balance']):
                                print('Insufficient balance',b1['balance'])
                                return
                            else:
                                # transfer the money
                                b1['balance'] = float(b1['balance']) - float(amount)
                                balance['balance'] = float(balance['balance']) + float(amount)
                                print('Your remaining balance is:',b1['balance'])
                                # change password status
                                pwd['status'] = 'Closed'
                                return
                        else:
                            print('Inavlid PIN')
```

```
            print('Inavlid account number')

    print("Invalid Password")


def check_pin(pin):

    """fucntion for checking customer pin number"""

    for customer in customers:
        if customer['pin'] == pin:
            return True
    return False


def get_balance(pin):

    """Return a balance ofcustomer """

    # generate symmetric key for encrypting user password
    key = Fernet.generate_key()
    cipher_suite = Fernet(key)

    for bal in balances:
        if bal['pin'] == pin:
            return bal['balance']


# entry fucntion
menu()
```


End of the Document