Addis Ababa University

Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

Secured and Usable Framework Design for Mobile Financial Service

BY: ASRAR MOHAMMED

A Thesis submitted to School of Electrical and Computer Engineering

In Partial Fulfillment of the Requirements for the Degree of

Master of Science in Telecommunication Engineering

Addis Ababa, Ethiopia

November, 2018

Declaration

I, the undersigned, declare that the thesis comprises my own work in compliance with internationally accepted practices; I have fully acknowledged and referred all materials used in this thesis work.

Asrar Mohammed

Name

Signature

Addis Ababa University

Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

Telecommunication Engineering Graduate Program

This is to certify that the thesis prepared by **Asrar Mohammed**, entitled *Secured and Usable Framework Design for Mobile Financial Service* and submitted in partial fulfillment of the requirements for the degree of Master of Science in Telecommunication Engineering (Telecommunication Information Systems Track) complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the Examining Committee:

Dr. Yalemzewd Negash		
Chair of School Dean	Signature	Date
Dr. Murad Ridwan		
Advisor	Signature	Date
Dr. Yalemzewd Negash		
Examiner	Signature	Date
Dr. Surafel Lemma		
Examiner	Signature	Date
Director of Post Graduate Program	Signature	Date

ABSTRACT

All systems do not require security at the same level. Sensitive information such as financial transactions require higher level of security in terms of confidentiality, integrity and availability. Mobile Financial Service (MFS) is making financial transaction using mobile devices. Due to the inherent nature of MFS using wireless technology, it makes the service susceptible to different attacks. Currently, in Ethiopia mobile financial service is mostly being provided using Unstructured Supplementary Service Data (USSD) technology. This study first identified many vulnerabilities and possible attacks that can be made on the current scheme by reviewing existing literatures. On top of this, analysis of existing MFS technologies has been made. Accordingly, Subscriber Identification Module (SIM) based approach is suggested since it is more applicable for the case of Ethiopia. The newly designed framework is found to be better than the original model in terms of security (confidentiality and integrity). The study further investigated usability of the existing and newly proposed models' user interface with a sample of 37 experts from ethio telecom and Commercial Bank of Ethiopia. Results from the experiment indicate that the current scheme took statistically significant time to complete a given task than the proposed model. The current model is preferred by participants on some of usability parameters such as learnability, satisfaction and ease of use. Overall, 94.6% of the experts involved on the experiment preferred the proposed model due to its security (better authentication using One Time PIN (OTP) code).

KEYWORDS

Usability and Security, USSD, Mobile Banking Security, Secured Framework, Mobile Financial Service

ACKNOWLEDGMENTS

First of all, I would like to say “Al-hamdu lillahi rabbil ’alamin” (All the praises and thanks be to Allâh, the Lord of the Universe) for everything. Second, I would like to thank my advisor, Dr. Murad Ridwan, for his supervision, guidance, and valuable feedback throughout this thesis work.

I also would like thank all my colleagues from ethio telecom information system department, IT expert from Commercial bank of Ethiopia especially Mr. Mesfin Belay and Mobile and Internet Banking Manager Mintesinot Siyum, who provide me valuable information and participated in doing the usability experiment.

My special thanks goes to my entire family for their patience during the research work and encouraging me through moral support. Specially I would like to thank my respected wife Zebiba Hussien and my lovely daughters Tesnim Asrar and Sidra Asrar.

The last but not the least, I would like to thank my company ethio telecom for giving me this opportunity and every support provided during my stay at the University.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

2G	Second Generation Mobile
3G	Third Generation Mobile
4G	Fourth Generation Mobile
AES	Advanced Encryption Standard
BSC	Base Station Controller
CBE	Commercial Bank of Ethiopia
DES	Data Encryption Standard
DOS	Denial of Service
EIR	Equipment Identity Register
GSM	Global System for Mobile communication
GSMA	Global System for Mobile communication Association
IBE	Identity Based Encryption
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ISO	International Standard Organization
ITU	International Telecom Union
IVR	Interactive Voice Response
MAC	Message Authentication Code
MFS	Mobile Financial Service
MNO	Mobile Network Operator
MS	Mobile Station
MSC	Mobile Switching Center
MSISDN	Mobile Station International Subscriber Directory Number

NIST National Institute of Standards and Technology

NSS Network Switching Subsystem

OTA Over the Air

OTP One-Time Password

PIN Personal Identification Number

PKI Public Key Infrastructure

SAT SIM Application Toolkit

SIM Subscriber Identification Module

SMS Short Message Service

SOA Service Oriented Architecture

SS7 Signaling System 7

STK SIM Toolkit

UI User Interface

USSD Unstructured Supplementary Service Data

UX User Experience

VAS Value Added Service

VLR Visitor Location Register

VPN Virtual Private Network

WAP Wireless Application Protocol

WML Wireless Markup Language

1

INTRODUCTION

The number of mobile service subscribers is assumed to increase from time to time. Based on facts obtained from website of ethio telecom, the sole telecom service provider in Ethiopia, currently, the total number of mobile customers reached to 65.7 million [1]. This large number of customers can be a base for different kinds of services to emerge. One of these services can be MFS, which refers to making banking and other financial transaction such as balance enquiry, withdrawal, fund transfer and effecting payment using a mobile device from anywhere and at any time via mobile network [2].

MFS has become an important driver of financial inclusion in a growing number of countries. They are bringing finance to the unbanked (people without bank account at a financial institution). Ethiopia is among six countries in the world having economies with half or more of adults unbanked [3].

MFS in general and mobile banking in particular is more relevant to Ethiopia since it has a large number of unbanked population [3]. According to National Bank of Ethiopia quarterly report for 2017/2018, one branch in Ethiopia serves 21,651 people on average and of the total 4,257 branches of which 34 percent is located in Addis Ababa [4]. Mobile Financial Service such as mobile banking has significant contribution in banking the unbanked society which has an impact on the national economy, though there are challenges on adoption of the service from customer side. For instance, based on report from internal source, only 10 percent of the total customers use mobile banking in the case of commercial bank of Ethiopia.

Many researches have been made to identify the cause of low mobile banking adoption rate in different countries [5], [6], [7]. Like in many other countries the main reasons in the case of Ethiopia is the perceived notion of lack of security and ease of use [8], [41]. One of the main ways to clear out the perception is by

conducting assessment on existing infrastructures and services used for mobile banking.

This research will address security and usability issues on current mobile financial service from operator side in this case ethio telecom.

1.1 STATEMENT OF THE PROBLEM

The main platform used for mobile banking in Ethiopia is USSD. Ethio Telecom uses USSD platform to provide interactive menu based service for all kind of mobile financial services. The same platform has been used to transact financial information even by ethio telecom for air time recharge and transfer.

Several studies [9], [10], [11], [12], [13] indicate that every USSD information is visible inside the operator's network including sensitive information such as Personal Identification Number (PIN), which is used for mobile banking service authentication, stored in clear text format in USSD gateway. The visibility of PIN and other sensitive information in plain text both within the network and in the servers' log file is a breach to security with respect to confidentiality and privacy. Furthermore, the current platform does not guarantees the non-alteration (modification, addition, or deletion) of the message in the middle of communication between the user and service provider.

On the other hand, the current USSD based platform operate in such a way that every communication whether legitimate or not will be forwarded to MFS service provider. This will make the service providers' system vulnerable to Denial of Service (DOS) attack.

In general, the current platform is not secured enough for sensitive information such as mobile banking as it lacks confidentiality and integrity besides making the service provider's system vulnerable to DOS attack.

This research analyzes MFS technology options and attempts to addresses the problem of confidentiality and integrity through proposing a new framework. Besides,

maintaining the usability advantage of USSD based approach.

1.2 OBJECTIVE

1.2.1 *General Objective*

The main objective of the study is to explore technologies for mobile financial service applicable to Ethiopia and design a framework which is secure in terms of confidentiality and integrity while maintaining or improving the usability as compared to the current model.

1.2.2 *Specific Objectives*

The specific objectives of the research are:

- Explore and understand the subject matter through literatures.
- Identify security concerns related to the current mobile financial service platform from telecom service providers' side.
- Identify mobile financial service technology options applicable for Ethiopia
- Propose a framework that will resolve the current problem.
- Develop, test and analyze the prototype based on international standards both from security and usability aspects.
- Report the result of the study and give recommendation on future works.

1.3 SCOPE AND LIMITATIONS

1.3.1 *Scope of the Study*

This research focuses on designing a mobile financial service which is more secured and usable as compared to the current platform (USSD). The security issues such as authentication, confidentiality and integrity have been considered on this

study. Furthermore, this thesis attempted to mitigate the problem of availability issue that could occur on service providers side whenever user frequently attempt to access their system without being registered.

This study does not deal with availability from Mobile Network Operator (MNO) point of view. Since it require separate security mechanism from the one we use for confidentiality and integrity and it also need further checking to figure out exactly where the problem is.

1.3.2 *Limitation of the Study*

The main challenge we faced during this research is lack of tool used for manipulating SIM card, which can be a reader. The result would have been more comprehensive, had it been we used the tool so as to investigate the feasibility of designing a more advanced and usable model like Public Key Infrastructure (PKI) security technique on existing SIM card.

1.4 CONTRIBUTIONS OF THE RESEARCH

Nowadays, security is a big concern for many services provided through internet or other networked environments. Especially when it comes to financial transactions, security is indispensable requirement that need to be checked for a system to be functional. Hence, this research explored technology options applicable for Ethiopia and design the framework which is far more secured and usable as compared to the existing USSD based platform.

The results and findings from this research will greatly benefit the telecom industry in general and ethio telecom in particular in terms of identifying security vulnerabilities on the USSD based platform, exploring the appropriate technology to be used and suggesting the possible framework on which the mobile financial service shall operate.

The service providers can also benefit from this study since the main cause for the low adoption rate is security and usability (ease of use). Hence, having solution

on these regard is assumed to improve the adoption rate and be a reason for customer satisfaction and increased revenue through more service usage.

Furthermore, this study can be used as an input for other similar research in the area of mobile financial service security and usability.

1.5 METHODOLOGY

1.5.1 *Literature Review*

In order to identify, analyze and propose the appropriate solution different mobile financial service technologies have been explored through reviewing existing literatures which include journal, magazine, articles, thesis, books, conference papers, white papers and international standards.

Review of existing literatures also used to identify related works on the area of mobile financial service security and usability as well as the methodology being followed. Beside this, concepts on security and usability are explored from literatures and taken as an input during the design, analysis and evaluation process.

1.5.2 *Data collection*

We conducted a survey mainly on usability attributes and provided questionnaire to participants and asked them to rate their level using a five-point Likert scale. Most of the questions in the survey questionnaire were closed-end type. The survey was prepared together with user interface designed using android studio to simulate both SIM based and USSD based solutions.

1.5.3 *Experiment*

1.5.3.1 *Experiment Setup*

Experimental study conducted to evaluate the current and proposed model UI from usability point of view. Information system experts from ethio Telecom and

Commercial Bank of Ethiopia, the state owned bank in Ethiopia with large number of customers, are involved on this experiment.

The experiment is implemented in such a way that two interface designed using android studio. The first one for USSD based and the other one for SIM based. USSD based flow is designed based on CBE-Birr, a mobile banking solution developed by Commercial Bank of Ethiopia. On the other hand, the SIM based interface designed based on our proposal to make the user interaction easy through reducing user interaction and applying recommendation discussed on literatures [14], [15].

1.5.3.2 *Participants*

A total of thirty-seven participants involved in this experiment. Twenty-five of them are experts from Ethio Telecom technical team working on design, operation and value added services. Experts from mobile financial service providers such as Commercial Bank of Ethiopia (CBE) constitute a total of twelve participants.

Questionnaires were prepared based on the literature review on usability. The first part of the questionnaire included profile information about respondents' education level, job title, whether he/she is using mobile banking or not. The purpose of these profile information is in order to see the level of experience and domain of the participant. On the other hand, usability for both platforms have been evaluated based on usability elements defined by ISO and other prominent experts on usability. These elements include: efficiency, effectiveness, satisfaction, ease of use and learnability.

1.5.3.3 *Procedure*

The tasks for this scenario were derived from USSD based CBE birr mobile banking application. Accordingly, send money operation is selected for this purpose as it has many activities within it and helps to show the user interface in different way.

To obtain the widest possible range of responses from technology or service

providers, such as banks and experts from ethio telecom design, project and operation team employees have been involved on the experiment. The collected data were then analyzed using statistical methods. Three PINs are selected in such a way that the first PIN is simple and easy to remember where as the second and third PINs are relatively complex. Plain PIN is ued for USSD experiment whereas one-time PIN code, which is derived from the PIN code string received from service provider have been used for experimenting SIM based interface.

Authentication for SIM based UI is based on One-time PIN code scheme and the steps to be followed are provided to the users beside the support given during the experiment.

Participants do the experiment three times for each of the User Interface (UI) so as to see the learnability and the effect of PIN complexity on efficiency.

We have used two timers to record the total time taken for the send money operation to complete both in the case of USSD based UI and SIM based UI. Beside this, authentication time is also recorded in order to see the effect of One Time PIN code in terms of time taken.

1.5.4 *Tools and Techniques*

In this study, we have used tool such as Java technology using Net-Beans for server side and WML technology using WAC for client side application development. These tools have been selected based on suggestion by other researchers on similar area. Beside these, we used android studio to design and develop the UI for both SIM based and USSD based approach. Statistical tools and techniques have been used to analyze the result of experiment and data collected through questionnaire.

1.6 THESIS ORGANIZATION

Chapter 2 discusses background information on mobile financial service and the technologies being used to provide the service followed by concepts about security and usability. In Chapter 3 review of related works presented in three parts

the first from security aspect, the second from usability point of view and finally on methodology and approach. Chapter 4 discusses the proposed design and prototype development. Chapter 5 presents the result analysis and discussion. Finally, Chapter 6 provides conclusion and future works.

2

LITERATURE REVIEW

2.1 BACKGROUND

According to world bank global findex report, Globally, nearly 1.7 billion adults remain unbanked; without an account at a financial institution or through a mobile money provider. Because account ownership is nearly universal in high-income economies, virtually all these unbanked adults live in the developing world. The Unbanked adults are more likely to have low educational attainment [3].

On the other hand, number of mobile subscribers has been growing at an amazing rate worldwide. According to Global System for Mobile communication Association (GSMA), there are 5 billion unique mobile subscribers [16]. This high growth rate is also happening in Ethiopia, where, the current mobile subscribers reached to 65.7 million which can be one of the reason for the emerging value added services such as mobile financial service [1].

2.2 MOBILE FINANCIAL SERVICE

MFS refers to making financial transactions such as balance enquiry, fund transfer and making payment using a mobile device from anywhere and at any time via mobile network.

There are two models for mobile financial service bank-led and non-bank led. The bank - led model is the most common in developed countries and serves mainly the citizens who already have a bank account. In non- bank led model agents such as value added service providers like the case of M-Birr and HelloCash in Ethiopia and famous M-Pesa in Kenya provide banking service using mobile network. In this model banks play only a supporting role. In the other hand, both models rely

on mobile network to operate. Hence, mobile network play vital role in providing mobile financial services.

2.3 OVERVIEW OF GSM NETWORK

Global System for Mobile communication (GSM) is a standard to describe the protocols for second-generation digital cellular network. The GSM network architecture consists of different elements that all interact together to form the overall GSM system.

The GSM network architecture as defined in the GSM specifications can be grouped into four major subsystems [17]:

- Mobile station (MS)
- Base-Station Subsystem (BSS)
- Network and Switching Subsystem (NSS)
- Operation and Support Subsystem (OSS)

A generic diagram of the overall GSM system architecture with these four main functional units is shown below:

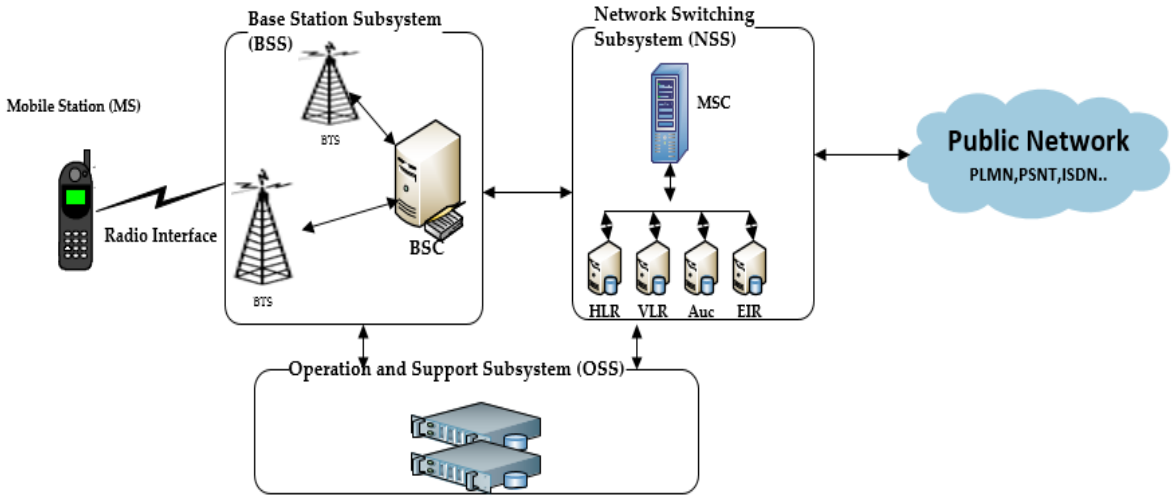

Figure 2.1: GSM system architecture

2.3.0.1 *Mobile station*

Mobile Station (MS), provides the air interface to the user in GSM networks. It consists of main physical equipment such as mobile phones and SIM card.

It also contains a number known as the International Mobile Equipment Identity (IMEI) which is used by a GSM network to identify valid devices. The number is usually unique and embedded in the phone at manufacture and "cannot" be changed [17]. It can be used by the network during registration to check whether the equipment has been reported as stolen.

The SIM contains International Mobile Subscriber Identity (IMSI) which is a unique number to identify GSM subscriber on the network [17].

2.3.0.2 *Base Station Subsystem (BSS)*

It is fundamentally associated with communicating with the mobiles on the network. This subsystem consists of a base station controller and one or more base transceiver station [17]:

Base Transceiver Station (BTS): The BTS used in a GSM network consists of the radio transmitter receivers, and their associated antennas that transmit and receive to directly communicate with the mobiles.

Base Station Controller (BSC): This element controls a group of BTSs, and is often co-located with one of the BTSs in its group. It manages the radio resources, allocate channels and controls handover within the group of BTSs.

2.3.0.3 *Network Switching Subsystem (NSS)*

This subsystem also called GSM core network provides the main control and interfacing for the whole mobile network. It consists of five major components:

Mobile Switching Centre (MSC): The MSC mainly acts as a switching node. It also provides additional functionality such as registration, authentication, call location, inter-MSC handovers and call routing to a mobile subscriber. In addition to these, It acts as an interface to the PSTN so that calls can be routed from the

mobile network to a phone connected to a landline [17].

Home Location Register (HLR): One of the major database that contains all information about each subscriber along with their last known location. So that, the GSM network is able to use the information to route calls to the relevant base station.

Visitor Location Register (VLR): VLR contains the exact location of all mobile subscribers currently present in the service area of the MSC. It assigns a Temporary Mobile Subscriber Identity (TMSI) that is used to avoid using IMSI on the air.

Equipment Identity Register (EIR): This is another database that keeps the information about the identity of mobile equipment such the International mobile Equipment Identity (IMEI) that reveals the details about the manufacturer, country of production, and device type. The EIR is the entity that decides whether a given mobile equipment may be allowed onto the network.

Authentication Centre (AuC): The AuC is a protected database that contains the secret key which is also available in the subscriber's SIM card. It is used for authentication and encryption of communication on the radio channel.

2.3.0.4 *Operation and Support Subsystem (OSS)*

This subsystem is another element within the overall GSM network architecture that is connected to components of the NSS and the BSC. It is used to control and monitor the overall GSM network and it is also used to control the traffic load of the BSS [17].

2.4 TECHNOLOGIES FOR MOBILE FINANCIAL SERVICE

Mobile network is a backbone of mobile financial services. It support different technologies to be used as a channel so as to link service requester and service provider. In General, technologies used for mobile financial service can be classified into two major categories: server side and client side. Server side technology options are those that do not require client application to be installed on consumer's SIM or mobile handset. Such channel can be SMS, IVR, USSD and WAP and

client side are those applications built or embedded on a consumer SIM or mobile handset. Examples of client-side applications are STK and mobile applications [18]. Each of these technologies are briefly described below.

2.4.1 *Short Messaging Service*

Short Message Service (SMS) is a GSM standard known with the characteristics of store and forward principles that means the message will first arrive on SMS center before reaching the intended customer. This technology has limitation on the number of character to send and receive at a time which is a maximum of 160 characters long. Mobile financial service using SMS requires a registered customer to initiate a transaction by sending a structured message to the service provider. This structured message can be defined based on service providers interest mostly requires a tag word identifier to instruct the SMS gateway to submit the message to the correct SMS application. A SMS center stores and forwards the structured message to the gateway allocated to the short code used by the MFS provider.

The MFS provider would use the consumer's mobile number, forwarded by the SMS center with the structured message, to identify the consumer and respond to the consumer's request [18].

Using SMS for MFS has an advantage of being ubiquity (workable on most of the device and mobile network available) and inexpensive to deploy. However, SMS has many limitations in terms of security and usability [19], [20].

2.4.2 *Interactive Voice Response*

Interactive Voice Response (IVR) is a phone technology that allows a user, to interact to telephone system through a voice menu. The user receives pre-recorded prompts and responds by selecting keys such as "press 1 for yes, press 2 for no". It uses speech recognition technology to interpret the caller's simple spoken answer such as "yes", "no", or more complex words and sentences as a valid response to the voice prompt.

MFS using IVR requires a registered consumer to make a call to a published telephone number and be answered by a pre-recorded voice that presents various menu options to the consumer. The IVR system would then take the necessary instructions from the consumer by recording the tones of the number selections that the consumer enters on the key pad, or through spoken commands, and creates an instruction that is given to the service provider. The service provider would use the consumer's mobile number forwarded by the network operator to identify the consumer and as a factor of authentication [18].

IVR systems are more user friendly and secured as compared to SMS but relatively expensive to deploy and maintain [20], [18].

2.4.3 *Wireless Application Protocol*

WAP is a type of mini Internet experience designed for small mobile phone screens. It is used for transmission of simple web pages in primarily 2G networks and may contain links and icons formatted especially to be usable and visible on the small screen of the mobile phone [21].

WAP is an open international standard for applications that use wireless communication. WAP or mobile Internet banking offers a consumer a similar experience to that of Internet banking. The consumer would browse to a mobile Internet site by accessing the WAP browser on their mobile phone and entering the website address. The actual banking application resides at the bank and is secured and monitored in the same way as an Internet banking website [18].

2.4.4 *Mobile Applications*

Mobile applications for MFS can be applets (application developed using Java technology targeting feature phones) or more advanced applications designed for smart-phones MFS.

Technically, small Java 'applets' can be installed on compatible phones either via Bluetooth or Over the Air (OTA) using WAP. This method is similar in principle

to a smart phone application, but running on a less sophisticated type of handset operating system [21].

Nowadays, smart phone applications can provide a rich-media User Experience (UX) that utilize smartphone device features which include large color screens, touch access, faster access through 3G, as well as more context-sensitive access to MFS services. To a large extent, the interface is also dependent on sufficient bandwidth, which is largely lacking in rural areas of emerging markets [21].

2.4.5 *SIM Based Applications*

SIM based application can be developed using SIM Application Toolkit (SAT). SAT also known as SIM Toolkit (STK), like SMS, is a well proven GSM standard and mainly used for more advanced services that require high security [21], [18]. It consists of a set of commands programmed into the SIM card which define how the SIM should interact directly with the outside world and initiates commands independent of the handset and the network.

STK has been deployed by many mobile operators around the world for many applications, where a menu-based approach is required, such as mobile financial service and content browsing.

As with USSD, STK is especially prevalent in developing countries where entry-level basic and feature phones are mostly used. STK is currently one of the most extensively and globally used mobile interfaces in MFS other than USSD [21].

The major advantage of using STK for mobile financial service is being highly secured and network or device independent. An application developed using SIM Toolkit will work in the 3G networks as well as when roaming into a foreign 2G network.

The challenge in SIM based applications is uploading the application onto a SIM card which already distributed in the market. The MNO has the option of sending the application Over the Air (OTA), through the delivery of encrypted SMS mes-

sages that self-configure the application on the SIM or provisioning a new SIM card with the application already embedded within the SIM [18].

2.4.6 *Unstructured Supplementary Service Data*

USSD is a GSM communication technology for transmitting information over GSM signaling channels. Like SMS, it is used to send text only between a mobile phone and an application program in the network. But unlike the SMS, is not using the store and forward mechanism rather transactions occur real time during the session.

In its simplest definition, USSD 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. It is limited to transport a message of up to 182 alphanumeric characters between the mobile handset and the network.

USSD is as standard a feature as SMS and is available in an estimated 95% of handsets today. USSD requires no additional installation on the consumers SIM or handset and is already built into most GSM networks [18].

USSD technology mainly used channel for mobile banking in developing countries [13]. However, like SMS, it sends data in clear text over the network. Hence, it violet the confidentiality requirement for secured financial system [9], [10], [11], [12], [13], [22].

While the USSD specification allows a USSD session of up to 600 seconds, typical allowance by MNOs for MFS and other third-party services is up to 180 seconds, with 120 seconds being the typical maximum time allowed for the entire USSD session by MNOs [21].

In general, most of the above MFS technology options comprise only two components: a simple mobile phone application and a corresponding mobile transactions server. The server understands limited set of messages coming from phones, uses background financial data to perform transactions, and returns the result. Such

implementation cannot be easily extended with new functions, without modifying both client or server or both which is not efficient. Those systems do not scale, meaning that phone application, designed to access and use one server, cannot access and use any other mobile financial server. Finally, these systems cannot be interconnected, so that users registered in one system cannot transfer funds to and use functions of other systems [23].

2.5 COMPARISON OF MFS TECHNOLOGY OPTIONS

In order to compare MFS technologies listed under Section 2.4 the following parameters have been identified from literatures and analysis made for each of the technologies.

2.5.1 *Cost*

In our case, the cost element is considered only from MNO point of view which include cost of deployment and operational cost [18], [20].

2.5.2 *Phone Type*

Basic phones, also called 'low-end device', have limited feature sets and no or limited capability of installing third-party applications, and no or very limited data connectivity. They can, however, for the most part, access MFS platforms through the use of basic USSD and STK capabilities [21].

Feature phones relatively have more functions than basic phones, but limited functionality and proprietary operating systems (OS). They include most of the features of basic phones, augmented in many cases by features such as Bluetooth and MMS, which are mostly narrowband data connectivity options. They also include wireless application protocol (WAP) capabilities, and, in some cases, 3G capabilities [21].

Mobile device used by the customer determine the technology selection for MFS.

Checking the target market and their mobile device is important in determining the appropriate technology [18], [24], [20].

2.5.3 *Security*

Security is one of the vital requirement for MFS channel selection. It shall be checked from confidentiality and integrity point of view [18], [24], [20]. Generally, although they use encrypted SMS, Java-based MFS apps are more efficient and cheaper to operate than STK access to MFS. Java applets mostly use bank-grade encryption for SMS, though they are not designed for basic phone types [21].

2.5.4 *Usability*

The target customer literacy level and capability to use the technology shall be considered during technology selection for MFS [18], [24], [20].

2.5.5 *MNO Dependency*

The last but not the least MNO play an important role in channel selection. During channel selection the extent to which the technology depends on MNO need to be checked [18], [24], [20].

Summary of comparisons of technology options with respect to the above parameters are shown on Table 2.1. Accordingly, from technology options that does not require advanced handset such as SMS, IVR, USSD and SAT, SIM Application Toolkit(SAT) is secured. Though, mobile application is better in-terms of both security and usability, it requires advanced handset.

Table 2.1: Summary of comparison of MFS technology options

Technology Options	Handset Requirement	Security	MNO Dependency	Cost	Usability
SMS	Standard Handset	No	Medium	Low	Low
IVR		No	Medium	High	High
USSD		No	Medium	Low	Medium
SAT		Yes	High	Medium	Medium
Mobile Application	Advanced Handset	Yes	Low	Medium	High
WAP		Yes	Low	Medium	Medium

2.6 MOBILE FINANCIAL SERVICE IN ETHIOPIA

Ethio telecom is the one and only telecom services provider in Ethiopia. Ethio telecom have been doing many expansion projects to increase the customer base and quality of service for the last four years.

Recently, mobile banking services are introduced in Ethiopia with objective of creating cashless society and reaching unbanked rural people. Almost all of the banks have implemented mobile banking service.

Besides, there are companies like M-birr and Hello Cash engaged mainly on providing the technology for mobile banking services. All of these service providers use USSD as a channel to deliver MFS.

As shown on Figure 2.2, four major components are involved in mobile banking service using USSD. The access network linking between user and the core network; the USSD platform on which the main service being provided and lastly the MFS provider who defines the actual service presented to the users. MNO required an interface into the SS7 networks that could convert GSM USSD request

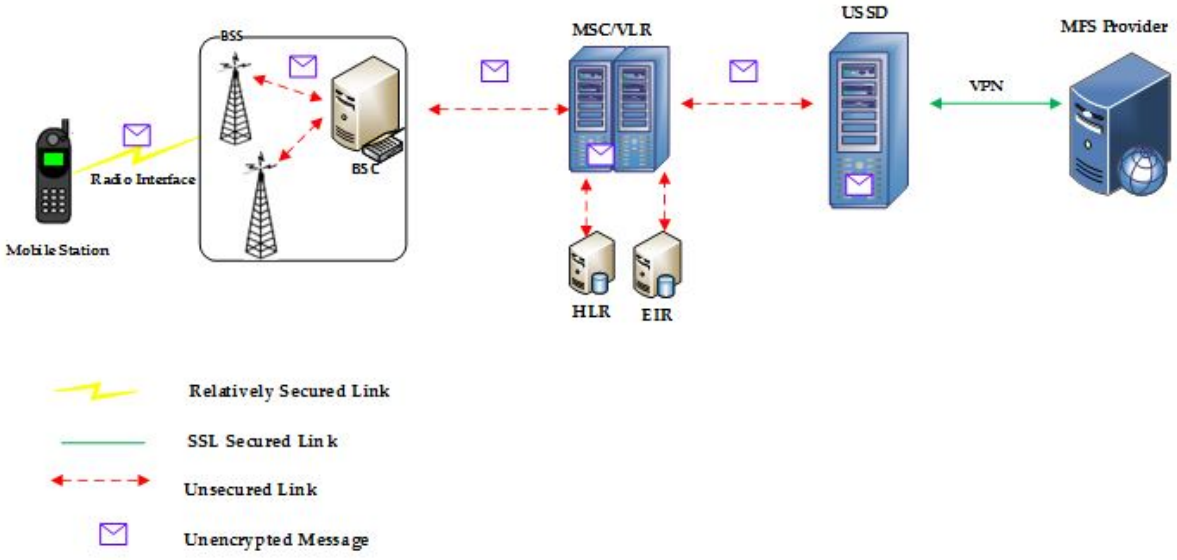

Figure 2.2: Current architecture of mobile financial service using USSD

response messages to the TCP/IP protocol so as that it can be send to third party application servers to process the requests. Generic flow of operations using USSD are listed below [18]:

1. A registered consumer would dial service provider's number mostly short code.
2. The consumer's request for the service would be passed through the network to the USSD gateway at the MNO, which in turn would recognize who the service provider is and forward the request to it.
3. The service provider would respond by forwarding to the consumer, through the MNO, a text based menu.
4. The consumer would receive this menu on their screen and enter the number based on their choice and follow the instruction.

2.6.1 *MFS Technology Option for Ethiopia*

In this research before designing a secured and usable MFS framework for the case of ethio telecom, investigation have been made on the current situation with respect to target customers.

Besides the access channel selection criteria pointed out above on Section 2.5, additional criteria have been explored such as literacy level, device type and mobile technology used by customers in order to select the appropriate technology.

2.6.1.1 *Technology Used by Customers*

Currently, based on report from ethio telecom internal source, from a total of 65.7 million customers, more than 50 million are still using 2G technology. This indicates that most of the customers are not ready for advanced service that require telecom network beyond 2G technology such as those that require high data rate.

2.6.1.2 *Mobile Device Share*

In Ethiopia based on source from ethio telecom, Most of the customers use basic and feature phone which constitute 68% of the total mobile device available on the network (Figure 2.3). Hence, the technology selection should mainly consider basic phones.

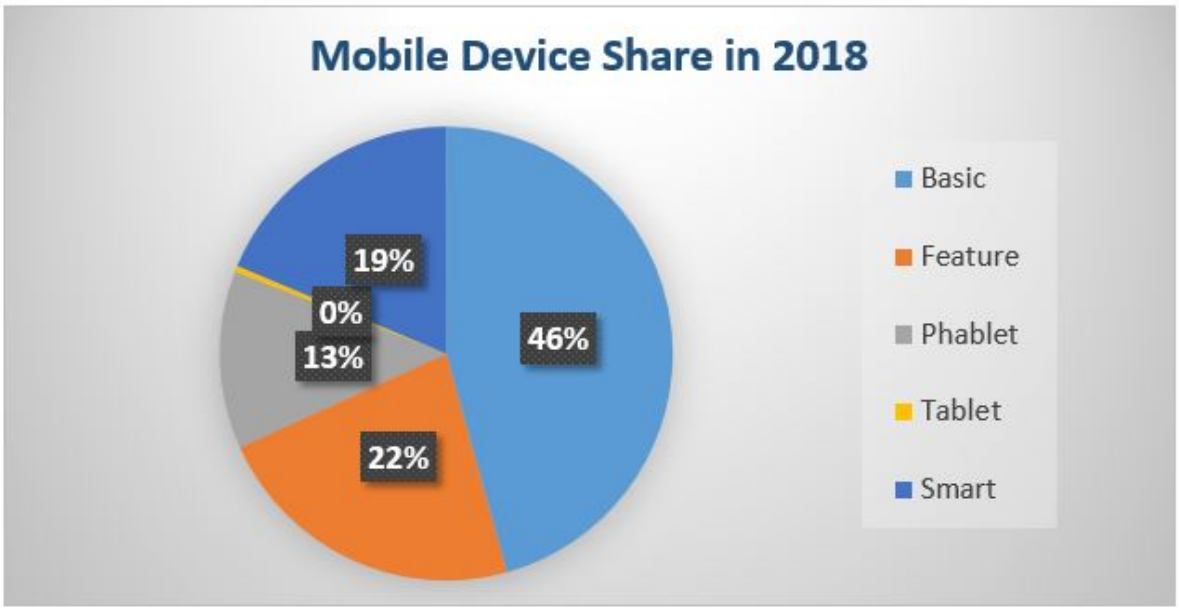

Figure 2.3: Mobile device share in ethio telecom network

2.6.1.3 *Literacy Level*

Based on The Global Findex Database, unbanked adults tend to have low educational attainment. Globally, 62 percent of the unbanked have a primary education

or less. This share is even higher in some countries, such as Ethiopia, where 92 percent of unbanked adults have a primary education or less [3].

Based on analysis of existing situations in Ethiopia in-terms of parameters presented on Section 2.5 and additional criteria discussed above, we proposed a SIM Application Toolkit technology to be used as a channel for MFS in ethio telecom. The reason can be, first of all, it is compatible on majority of the phone types including basic phones [21]. It is better with regard to security as compared to the other such as USSD. Furthermore, to some extent it has flexibility in-terms of designing UI which means we have room for making it usable. The last but not the least it can work on all types of mobile network technology 2G or 3G.

2.7 THEORETICAL BACKGROUNDS ON SECURITY AND USABILITY

In this section discussion on theoretical backgrounds regarding security and usability issues in general and their application and implementation on MFS in particular have been made.

2.7.1 *Security Objectives*

Security broadly defined as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability [25].

Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization [26]. International organization such as ISO and NIST recognized these three elements of the triad as the most crucial components of security. And hence they are considered as security objectives or goals that need to be met in order for a system to be secured.

1. **Confidentiality** Confidentiality is the property whereby sensitive information is hidden from unauthorized parties while being available to the right people. Secrecy is a term that is often used synonymously with confiden-

tiality. Confidentiality using cryptography is achieved using encryption to render the information unintelligible except by authorized entities. The information may become intelligible again by using decryption. In order for encryption to provide confidentiality, the cryptographic algorithm and mode of operation must be designed and implemented so that an unauthorized party cannot determine the secret or private keys associated with the encryption or be able to derive the plaintext directly without using the correct keys [25].

Data encryption is a common method of ensuring confidentiality. PIN and passwords constitute a standard procedure; two-factor authentication is becoming the norm. Other options include biometric verification and One time PIN such as security tokens or soft tokens [26].

2. **Integrity** Data integrity is a property whereby data has not been modified in an unauthorized manner since it was created, transmitted or stored. Modification includes the insertion, deletion and substitution of data. Cryptographic mechanisms, such as MAC or digital signatures, can be used to detect both accidental modifications such as those that sometimes occur during noisy transmissions or by hardware memory failures and deliberate modifications by malicious people. Non-cryptographic mechanisms are also often used to detect accidental modifications, but cannot be relied upon to detect deliberate modifications [25].

3. **Availability** The information created and stored by an organization needs to be available to authorized users and applications information is useless if it is not available. Information needs to be changed constantly, which means that it must be accessible to those authorized to access it.Unavailability of information is just as harmful to an organization as a lack of confidentiality or integrity. Imagine what would happen to a bank if the customers could not access their accounts for transactions [27].

2.7.2 *Security Attacks*

The three goals of security (confidentiality, integrity, and availability) can be threatened by security attacks.

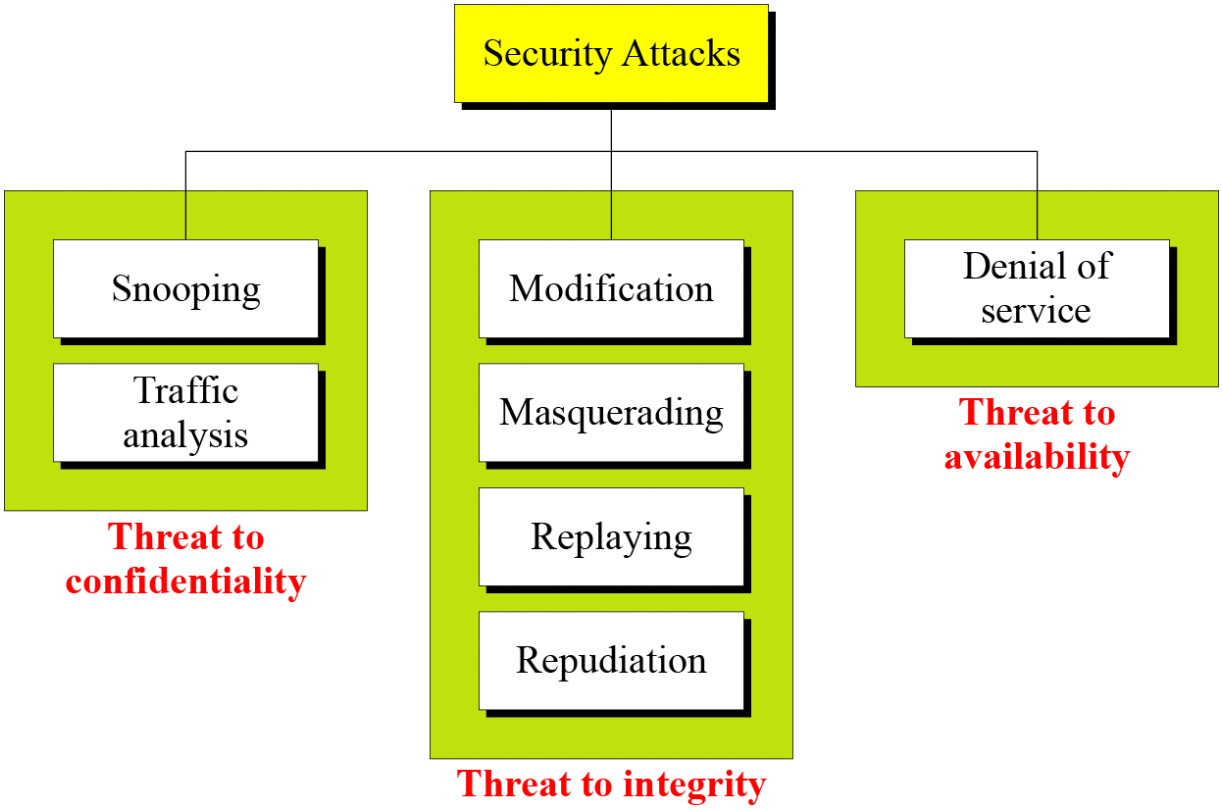

Figure 2.4: Taxonomy of attacks with relation to security goals[28]

2.7.2.1 *Attacks Threatening Confidentiality*

Snooping refers to unauthorized access to or interception of data. For instance, a transaction transfered through USSD channel may contain sensitive information such as PIN. An unauthorized entity may intercept the transmission and gets the PIN for later use. To prevent snooping, the data can be made hidden to the interceptor by using cryptography [28].

Traffic analysis refers to obtaining some other type of information by monitoring online traffic. Although, encipherment of data may make it non-intelligible through using cryptographic technique, the interceptor may still use the traffic to get some other critical information[28].

2.7.2.2 *Attacks Threatening Integrity*

Modification means that the attacker intercepts the message and changes it. For example, a customer sends a message to a bank to do some transaction. The attacker intercepts the message and changes the type of transaction to benefit himself/herself [28].

Masquerading or spoofing happens when the attacker impersonates somebody else. For example, an attacker might steal the bank card or PIN of the bank customer and pretend that heis that customer. Sometimes the attacker pretends instead to be receiver entity. For instance, a user tries to contact a bank, but another site pretends that it is the bank and obtains some information from the user [28].

Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it. For example, a person sends a request to her bank to ask for payment to the attacker, who has done a job for her. The attacker intercepts the message and sends it again to receive another payment from the bank [28].

Repudiation: This type of attack is different from others because it is performed by one of the two parties in the communication: the sender or receiver. The sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message. For example, a mobile banking user might request for his/her bank to send money to third party but later denying that she/he has made such request [28].

2.7.2.3 *Attacks Threatening Availability*

Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.

2.7.3 *Security Mechanisms*

Security mechanisms are technical tools and techniques that are used to implement security services. A mechanism might operate by itself, or with others, to provide a particular service. Some of common security mechanisms are as follows[29]:

2.7.3.1 *Cryptography*

Cryptography is the major technique to be used while transferring private information and data through open network communication, so that only the receiver who has the secret key can read the secret messages which might be documents, images or other forms of data.

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. In addition, Cryptography is also known as the science of secret writing. The goal of cryptography is to make data unreadable by a third party.In a high level it can follow the following simple steps:

1. The sender converts the plaintext message to ciphertext. This part of the process is called encryption (encipherment).
2. The ciphertext is transmitted to the receiver.
3. The receiver converts the ciphertext message back to its plaintext form. This part of the process is called decryption (decipherment).

Cryptography algorithms are divided into symmetric (secret-key) and asymmetric (public-key) network security protocols. Symmetric algorithms are used to cipher and decipher original messages (plain text) by using the same key. While Asymmetric algorithms uses public-key cryptosystem to exchange key and then use faster secret key algorithms to ensure confidentiality of stream data. In Public-key encryption algorithms, there is a pair of keys, one key is known to the public, and is used to encrypt information to be sent to a receiver who owns the corresponding private key. The private and public keys are both different and need for key exchange [28].

Symmetric Key Cryptography Since traditional ciphers are no longer secure, modern symmetric-key ciphers have been developed. Modern ciphers normally use a combination of substitution, transposition and some other complex transformations to create a cipher text from a plaintext. Modern ciphers are bit-oriented (instead of character oriented). The plaintext, cipher text and the key are strings of bits. Two examples of modern symmetric-key ciphers: DES and AES [28].

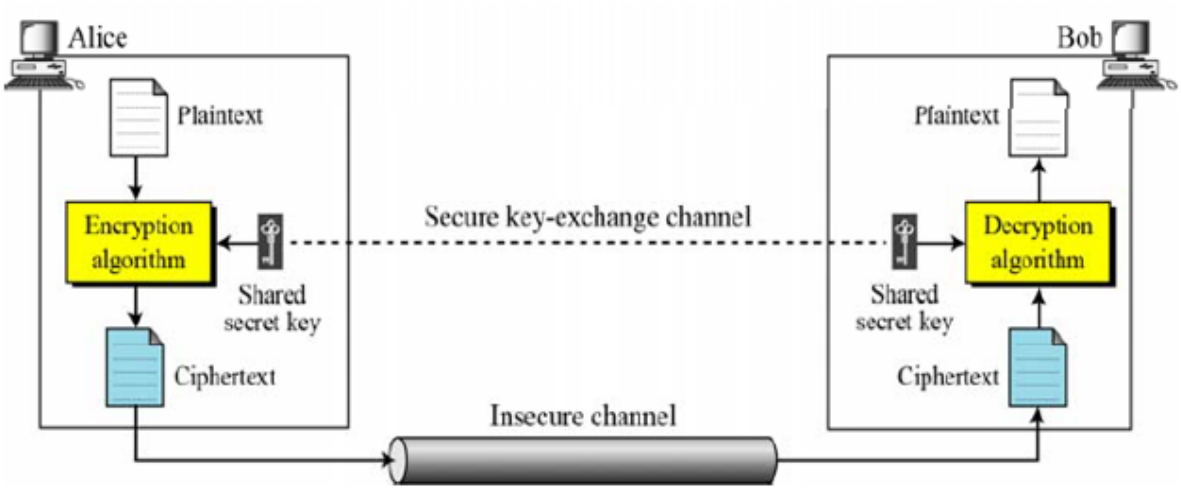

Figure 2.5: The general idea of symmetric-key cryptography [27]

Data Encryption Standard

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in 1977. DES has been the most widely used symmetric-key block cipher since its publication[27]. However, later it is replaced by triple DES to resolve the security drawback identified.

Advanced Encryption Standard

The AES is a symmetric-key block cipher published by the United State NIST in 2001 in response to the shortcoming of Data Encryption Standard (DES).

Asymmetric key Cryptography also know as public-key algorithm. Unlike symmetric key cryptography, there are distinctive keys in asymmetric-key cryptography: a private key and a public key. If encryption and decryption are thought of as locking and unlocking padlocks with keys, then the padlock that is locked with a public key can be unlocked only with the corresponding private key [28].

In general, cryptography plays vital role in the security to maintain the confidentiality, authentication, integrity and non-repudiation of the information; and the encryption is the backbone of cryptography.

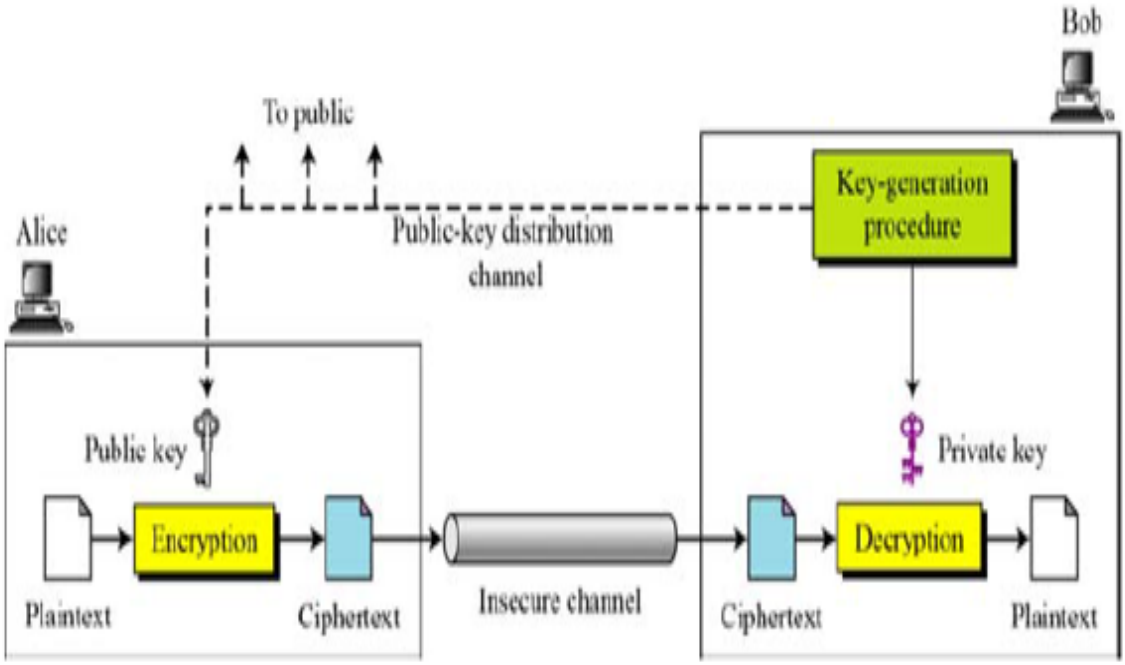

Figure 2.6: The general idea behind asymmetric-key cryptography [27]

Authentication is the process of proving one's identity. In other word, the property of knowing that the sender of the data is the actual sender is authentication. It is used to verify the identity of a user, device or other entity in a computer system. With authentication we can verify the user, device or any other entity in a system and it is often used as a prerequisite for allowing access to resources in a system. Initially, only one factor was utilized to authenticate the user. One factor authentication can be using a password or PIN to confirm the ownership of the user ID. However, this is assumed to be the weakest level of authentication. For instance, by sharing the password, one can compromise the account immediately. Moreover, an unauthorized user can also attempt to gain access by utilizing the dictionary attack or social engineering techniques. Commonly, the minimum password complexity requirement is to be considered while utilizing this type of authentication [30].

Further, it was realized that authentication with just a single factor is not reliable to provide adequate protection due to a number of security threats. As an intuitive step forward, Two-Factor Authentication was proposed that use password or PIN together with the factor of personal ownership, such as a smartcard or a phone.

Today, three types of factor groups are available to connect an individual with the established credentials [30], [31]:

- Something known. This is a secret known only by the claimant that can be checked by the verifier. Examples are a password, a PIN, a secret key and a private key.
- Something possessed. This is something that can prove the claimant's identity. Examples are a passport, a driver's license, an identification card and a credit card
- Something inherent. This is an inherent characteristic of the claimant. Examples are conventional signatures, fingerprints, voice, facial characteristics, retinal pattern and handwriting.

Subsequently, multi-factor authentication was proposed to provide a higher level of security. It uses more than two categories of credentials [30].

2.7.3.2 *Message Digests and Digital Signatures*

A message digest is a fixed size numeric representation of the contents of a message, computed by a hash function. A message digest can be encrypted, forming a digital signature. Messages are inherently variable in size. A message digest is a fixed size numeric representation of the contents of a message. A message digest is computed by a hash function, which is a transformation that meets two criteria [29]:

- The hash function must be one way. It must not be possible to reverse the function to find the message corresponding to a particular message digest, other than by testing all possible messages.
- It must be computationally infeasible to find two messages that hash to the same digest [29].

The message digest is sent with the message itself. The receiver can generate a digest for the message and compare it with the digest of the sender. The integrity of the message is verified when the two message digests are the same. Any tampering with the message during transmission almost certainly results in a different message digest.

A message digest created using a secret symmetric key is known as a Message Authentication Code (MAC), because it can provide assurance that the message has not been modified [29].

Message Authentication Code (MAC) is a simple short piece of information used to authenticate a message. It is a means to confirm that the message actually come from the right sender and has not been changed during the communication process. The MAC value is used confirm message's data integrity as well as its authenticity, by allowing the an entity who holds the secret key verify and detect changes if any on the content of the message.

2.7.4 *Definition of Usability*

The definition of usability according to Jacob Nielsen, well-known expert on Usability, is a quality attribute that assesses how easy user interfaces are to use. He emphasizes the word "usability" as a method for improving ease-of-use during the design process. He further points out five quality components which determine usability: Learnability, Efficiency, Memorability, Errors, Satisfaction [32]. On the other hand, International Standard Organization (ISO) defined usability as being a more comprehensive concept than is commonly understood by "ease-of-use". Their definition of usability is based on a context on which a product used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction [33]. This definition presents three components in the interaction that should be considered in a usability evaluation.

2.7.5 *Elements of Usability*

On the usability definition presented above, six elements are identified commonly by ISO and Jacob Nielsen. These elements include: Efficiency, Satisfaction, Effectiveness, Learnability, Memorability and Errors. Beside these elements, many other researchers [34], [35] identified some of these elements and additional more such as Simplicity, Comprehension ability, Learning performance.

In our study, some of the elements commonly identified and relatively applicable for our case are listed and discussed hereunder.

Effectiveness: the accuracy and completeness with which users can achieve their goals such as number of tasks performed. The measurement of effectiveness involves quality of solution and error rates.

Satisfaction: satisfaction is the user's experience and attitude toward the use of the system. Measurement of satisfaction can be conducted through questionnaires, interviews, or rating scales. One can ask question like how pleasant is it to use the design?

Efficiency: the rate in which how quickly users can perform the given tasks. The measurement of effectiveness involves criteria such as task completion time. Errors: how many errors do users make, how severe are these errors, and how easily can they recover from the errors?

Learnability: refers to the ability of the application to be easily learned by all levels of users one can ask question like How easy is it for users to accomplish basic tasks the first time they encounter the design?

Simplicity: refers to the state of being simple or easy to use.

In this study, we considered these elements both during user interface (UI) design process and evaluation to compare the existing and proposed UI.

2.8 SECURITY VULNERABILITY IN USSD

Vulnerability in security is a term used to refer to the weakness exhibited in the system that would lead to attack. Based on assessment made on the current USSD based mobile financial service platform, there are four vulnerability areas. Figure 2.7 shows area of concern on the generic USSD architecture. Details of each of these vulnerability areas are discussed as follows.

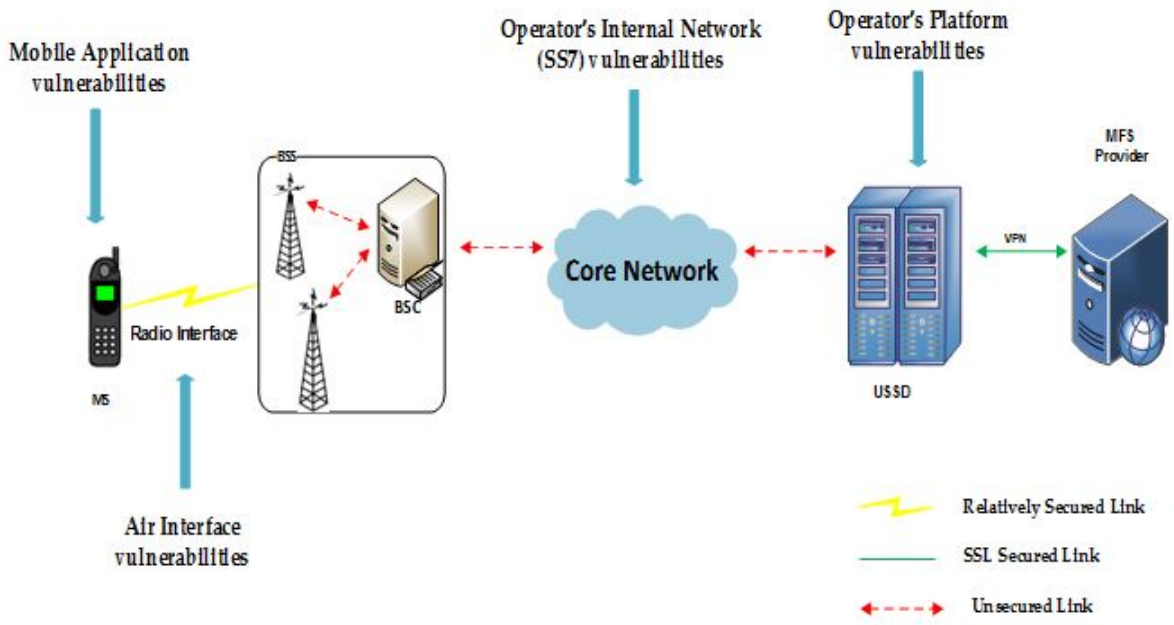

Figure 2.7: Security vulnerability in USSD based MFS

2.8.0.1 *Mobile Station Vulnerability*

End to end mobile banking security includes many stakeholders. If we start from end user side, we find that subscribers' mobile phone and applications that are used are of the areas of security concern. There are two types of applications when we consider mobile banking security. The first is the actual mobile application's security, which needs to go through rigorous tests to insure that it is not prone to security breaches.

In order to overcome security concerns of mobile applications, security tests need to be performed against applications and other involved components. Almost all the critical threats should be covered in this assessment. Individual components and security assessment with black box, gray box and white box approaches provides in-depth assessment [11]. This approach identifies vulnerabilities from the attacker's perspective.

The second is the installation of third party applications that are installed with or without the user's knowledge. Such applications could record user's credentials and compromise authentication security of end users. User's unawareness on smartphone might lead the user to install applications from untrusted sources. These applications might contain malware that can alter private information in the

smartphone or send private information to other devices [10]. Information sent by malware can later be used by an attacker to conduct fraud mobile financial transactions. In addition, mobile phone has several security features that by default are left by the manufacturer without being activated. Some of these features allow encryption of the data, but this task is left to the user. If such features are not enabled, the online interception of sensitive stored data such as user's PIN is possible by a third party [10].

2.8.0.2 *Air Interface Vulnerability*

End users access the mobile network with a combination of Subscriber Identity Module (SIM) and mobile wireless access channels. SIM cards are provided by ethio telecom. These cards are smart card, which contains a processor and non-volatile memory [36]. These cards have users' network authentication credential such as IMSI, authentication key (Ki) and encryption key (Kc). Test have shown that SIM cards can be successfully cloned. Memory capacity has advantages and disadvantages, which is 32KB SIM card Ki produced a success rate of 100 percent success, 64kb SIM card cloning success rate of 25 percent to 50 percent [36]. SIM cards can be cloned when subscribers lose mobile phone or at mobile service centers if SIM is provided along with phone. A loss of the aforementioned credentials will allow attackers to impersonate a user and conduct transactions on behalf of mobile banking users. This is due to the fact that a four-digit credential provided by banks can be easily obtained through brute force attack or dictionary attack.

Mobile access channel security relies on the strength of algorithm deployed in the network. GSM which is used by over 50M ethio telecom subscribers uses A3, A8 and A5 algorithms. The A3 and A8 cryptographic algorithms used in GSM are both implemented using a hash function known as COMP128; this makes them both rendered weak. COMP128's design was developed in secrecy violating Kerckhoffs' Principle. It was eventually reverse engineered at Berkeley in 1998 meaning that an attacker with access to a SIM card can determine the root key Ki. The key was successfully obtained by cryptanalysis of COMP128 performed by Briceno, Goldberg, and Wagner allowing the phone to be cloned [13]. An alleged seller, for example, could determine Ki using a SIM card reader before selling the phone.

The Ki and the IMSI can then be written by the attacker onto another SIM card which can be used to execute masquerading attacks.

Because of export restrictions on encryption technology, the stronger A5/1 ciphering algorithm is used only in Western Europe and a few others while the weaker A5/2 is used in central and Eastern Europe and other places where restrictions apply. As with COMP128; both of them violated Kerckhoffs' Principle and are both weak. A5/1 was cracked by Biryukov. The algorithm can be cracked using a moderate high performance PC only in few seconds. A5/2 also was cracked in less than a day using a method that requires only five clock cycles [13].

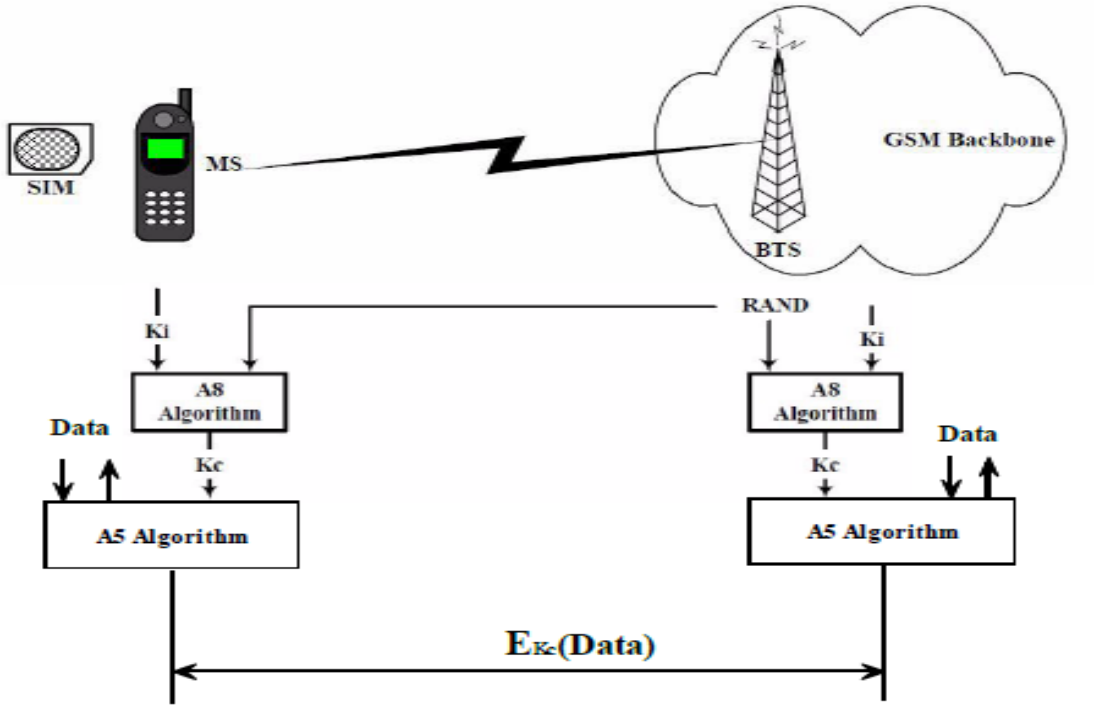

Figure 2.8: GSM A5 Encryption [13]

Another serious concern for GSM air interface security is the possible presence of fake base station. This is due to the fact that there is no mutual authentication in GSM. Only the subscriber is authenticated but not the base station in GSM. This lack of mutual authentication and the communication encryption being determined by only the base station are the two major flaws exploited by this attack [13]. Since the base station is in control for encryption; it enables the attacker to choose weaker encryption or none at all. By using fake base station, an attacker can convince the

mobile not to encrypt the communication and without being noticed executes a man-in-the-middle attack to make all communications go through him between the caller and the recipient [13]. As a result, an attacker can record all transactions and can conduct a chosen plaintext attack on the SIM by sending any RAND of its own choosing and obtain a corresponding SRES. It can thus achieve a SIM attack without even getting physical access to the SIM card [13].

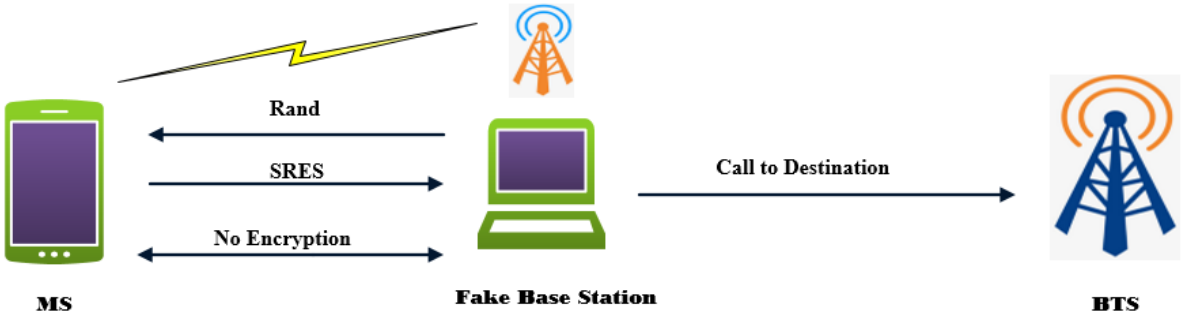

Figure 2.9: Fake base station [13]

2.8.0.3 *Operator Internal Network (SS7) Vulnerability*

After moving through the air interface, mobile banking data transverses through the operator's radio and core network before reaching the service providing platform. Encryption in GSM is only applied between the mobile and the base station; but across the rest of the network, no encryption is applied making data vulnerable when intercepted [13]. The protocol used for network nodes communication is signaling system number 7 or also known us SS7 . SS7 is a protocol which has been in used since the 1980s [37]. This protocol is based on the assumption it is run in trusted network. Keeping this in mind, no additional security layer is added in this protocol. Thus, data moves through the network in plain text format. It is after the BTS; the traffic is transmitted in plain text within the operator's network. If the attacker can access the operator's signaling network, he will be able to listen to everything that is transmitted, including the actual phone call as well as the RAND, SRES and Kc. This is achieved by creating fake MSC once an attacker gains access to the operator's network [37]. Access to operator's can be achieved through a number of ways. It is shown that it can be bought from Telcos with roaming agreements or roaming hubs for a few hundred euros a month,

some network operators are also known leave their equipment unsecured on the internet and Femtocells are part of the core network and have been shown to be hackable [37].

2.8.0.4 *Operator Platforms Vulnerability*

From operator's point of view another key concern is storage of data during translation between protocols and storage in the service giving platform. At USSD gateway, protocol translation is done from SS7 to TCP/IP implying that the message is in the clear at that moment in time [38]. We can thus see that there is a major exposure at the USSD gateway when the message protocol is converted from SS7 to TCP/IP. This is confirmed by conducting network trace between nodes as well as viewing logs on the USSD Gateway. It is thus becomes binding on the operator, to insure that USSD Gateway network trace as well as visibility of clear text are restricted so that the information trace is not exposed to the outside world [38]. This treats become reality when any attacker gets access to internal network or by operators' staffs. The connection after the operator's service platform is VPN connection between operator and bank which is secure.

2.9 SECURITY IN MFS TRANSACTION

Most of the current MFS technologies do not provide security features on their own. Security of these systems relies on features provided by the GSM network, which are not adequate, especially for financial transactions or on use of simple PIN schemes [23].

However, users will expect at least the same level of security that's available when banking on-line via their personal computer. In general both the real problem and the "perception" issue must be addressed in order to improve adoption of mobile financial services [39]. Accordingly, the following are some of the issues that need to be taken into account:

Data transmission must be secure: This is to mainly address the concept of confidentiality, which requires encryption of the connection between the device and the service provider.

Application and data access must be controlled: Before users can receive any sensitive information related to their bank accounts, a certain degree of verification must be completed. Ideally, the combination of several authentication factors and the possibility to challenge the user in case of a security breach should be part of the procedure.
Data integrity must be provided: Any sensitive data stored on the mobile device and communicated on the network must be protected against unauthorized modification. The issue of possible corruption and deletion error of information should also be considered in this regard.
Loss of device must have limited impact: The mobile financial service should be designed so that there will be limited impact when the mobile device is stolen.

2.10 GUIDELINES IN SECURITY AND USABILITY DESIGN

2.10.1 *Design for Security*

To improve the mobile financial service security and minimize the risks, International Telecom Union (ITU) recommends the design to ensure the realization of the following goals [40]:

- To reduce the possibility of interception of sensitive information during transaction.
- To reduce the possibility of retrieving sensitive information from databases
- To reduce the possibility of substitution or distortion of financial information during transaction;
- To reduce the possibility of using the system by unauthorized persons such as through masquerading by implementation of a unique authentication.
- To reduce the possibility of using "stolen" information which can happen after device lose.
- To provide a mechanism to make it impossible for participants to deny their actions after they have been involved.

- To make sure that all stakeholders involved on MFS comply with with legal rights and duties.
- To ensure the completion of transaction.

In order to achieve security goals, ITU further recommends all mobile financial system participants such as MNO and service providers to implement eight security dimensions in relation to the information being involved in the data exchange. Based on the implementation of this dimensions, ITU defined four security levels. The first four security dimensions are equally implemented at all security levels. While the rest four following have different implementation at different security levels [40]. The eight security dimensions are discussed hereunder

Access control: the access to each mobile financial system component must be granted based on end-user access level policy.

Communication security: to make sure delivery of messages in both directions so as to ensure the completion of a transaction.

Availability: ensures the preservation of authorized access to mobile financial system data and services. The requirement is applicable for all security levels and need to be met by the service provider.

Non-repudiation: this require a mechanism for preventing an individual or an entity from denying having involved in a particular action(for instance, sending money, paying bill).

Authentication: to ensure whether someone or something is who or what it claimed to be. Identity of the entities participating must be verified.

Data confidentiality: data communicated in the system shall be protected from being accessed or disclosed to unauthorized parties. Requirements to confidentiality are defined by the system data sensitivity.

Data integrity: this security service aimed at protecting data from unauthorized modification, creation, insertion, deletion and replay during the communication process.

Privacy: ensures the security of the information involved in the data exchange and stored by the system participants. The system participants shall mitigate against unauthorized data acquisition and transfer. In this regard, the system shall assure compliance with the financial industry standards .

2.10.1.1 *Security Levels*

According to ITU recommendation [40] there are four levels of security for mobile financial system. The level of security increase from the first to fourth. The recommendation further suggest that a secured mobile financial system need to satisfy level 3 to the minimum. Details on the levels of security are presented as follows:

1. Security level 1

   Mobile financial system can rely on the authentication of the client provided by the MNO. Data confidentiality and integrity are ensured by the communication environment. Besides, during storage and processing using security mechanisms of data storage and the system access control facilities. The privacy is ensured by avoiding sensitive data in the messages being transferred.

2. Security level 2

   In this level the improvement is on authentication where one-time-password or single factor authentication is used. Data confidentiality, integrity and privacy are ensured similarly to level 1.

3. Security level 3

   The system shall use more than one authentication factor to authenticate the client. Data confidentiality, integrity and privacy of a message shall be ensured by using security mechanisms such as encryption, data transfer protocols that ensure the security of the data being transferred. During data storage and processing, their confidentiality, integrity and privacy shall be ensured by additional mechanisms of encryption, masking and access control.

   To meet security requirements at this level, the system shall use special software applications, which need to be installed on clients' mobile devices. These applications shall implement two-factor authentication and ensure both

encryption and decryption of the transferred data. Each authentication shall require entry of the PIN or other activation mechanism to to activate the authentication key.

In this level, the security of data transferred over the communications channels shall be ensured by means of strong cryptography. The strength of a cryptographic method depends on the cryptographic key being used.

4. Security level 4
   This is the highest system security level. To meet the security requirements at this level, the system shall use hardware security modules installed in clients' mobile devices. These hardware security modules shall implement two-factor authentication and ensure both encryption and decryption of the transferred data. Each authentication shall require entry of the password or other activation data to activate the authentication key and the unencrypted copy of the authentication key shall be erased after each authentication. Both symmetric and asymmetric cryptographic algorithms are applied to message encryption. Implementation of other security dimensions shall fully correspond to level three.

2.10.2 *Design for Usability*

2.10.2.1 *Guidelines in Designing Usable User Interface*

During UI design process, list of characteristics proposed by Jailani et al. [14] is considered since it is identified specifically for mobile application and achieved a good result during evaluation. According to the author, usability elements listed under Section 2.7.5 such as effectiveness, efficiency,satisfaction and learnability can be achieved by adapting these characteristics:

- The interface shall be designed to perform one task at a time.
- The interface shall reduce the amount of input of text to a minimum by using features like combo box or filtering functionality to facilitate searches.
- The interface shall be designed to allow any action to be repeated or replicated easily.

- The application shall be designed to facilitate search and auto-complete.
- The interface shall be free from errors
- The interface shall be comfortable for the user to use.
- The application shall have the ability to facilitate the learning progress on how to use the application.
- It also must provide predefined list that are brief.
- The structure or flow of the application should not be too complex.
- The interface shall be consistent on all screens.
- The application shall use input method which are familiar.

Additionally, some more usability parameters that determine the quality of UI design are discussed in article [15] which includes:

- User control and freedom: Considering user's characteristics during design process.
- Error prevention or handling: The UI need to prevent users from going into an error prone state.
- Simple design and aesthetic: The design shall be ordered and appealing.
- Anticipation : Designing menu in a simple way through organizing item properly.

3

RELATED WORKS

In this chapter, related works of different researchers in the area of security and usability of mobile financial service were reviewed. The chapter is organized into sections which include related works from security perspective, related works from usability perspective and lastly the method and approach to design a secured and usable mobile financial service.

3.1 SECURITY

Many researches have been made in relation to securing mobile financial services. To the best of the researcher knowledge most of the study does not consider low end device such as basic phone in their design.The related works presented below designed a solution targeting mainly feature phones or smart phones.

G.Ramesh and F.Abadi [22] proposed security protocol using SMS and USSD that guarantees confidentiality, authentication, integrity and non-repudiation security services between client and server. Their solution is targeted to smart phone users. In terms of implementing end to end security, the researchers used a hybrid cryptographic scheme which combines the Identity Based Encryption (IBE) for digital signature, Advanced Encryption Standard (AES) algorithms for encryption, SHA256 hashing algorithm to generate a message digest and Lempel–Ziv–Welch (LZW) used to compress the SMS. The study also indicated that such solution requires processing capability from client side and does not apply for feature phone.

B.Belete in [41] proposed a conceptual framework which suggest the implementation of key authentication and message exchange mechanisms on both client and server. On top of this the research suggested one-time password as an additional security layer.However, this one time list of passwords are exchanged in a

printed format from service providers. The researcher further assessed the mobile banking service users' feedback through questionnaire after evaluating the model designed based on the proposed framework and found encouraging result such as improved perception in relation to risk of security. Beside this, the research indicated the need to assess the impact of such solution on usability or ease of use to the customers.

The study by A. Emmanuel [42] suggested using AES encryption algorithm using SMS as a channel between mobile device and server. Though this framework is designed for developing countries, it suggest to implement the solution using java application to be installed on feature phones.As part of the authentication improvement mechanism this researcher also proposed using one-time password. Similarly, article [13] proposed a model using AES algorithm to encrypt mobile transaction between client and server over SMS channel through installing Java based application on the client device. Beside the encryption, security mechanism such as message digest used to improve message integrity. The researcher also suggested to use PIN that include digit, character and symbols so as to increase the strength and propose mechanism to enforce users to change PIN periodically.

Apart from symmetric encryption key suggested by most of related works discussed above, reference [43], [19], [44] presented a model using PKI and found a better result in terms of security and user trust.

3.2 USABILITY

In reference [45] a study aimed at designing usable authentication for mobile banking is discussed. Accordingly, two prototype graphical and gesture password were developed and evaluated together with the existing PIN based authentication. The result of experimental study revealed that users' preferred PIN more than the other two.

Different form of One-Time Password (OTP) has been suggested by many researchers [41],[42],[46] ,[47].The concept in reference [46] and [47] are the same. Both of these paper presented on how users can drive one time PIN code from

a security string or nonce. In both case, nonces only contains digit from zero to nine and are used to encrypt PINs via substitution-based coding before either of them is transmitted to the bank server. However, both differ on the way they communicate security strings or nonces. The researcher in article [46] proposed a codebook which is similar in concept with EKO(an Indain based MFS provider) while the other researcher proposed a mechanisms to communicate by a server to the user right before authentication.In reference [46],the researchers indicated the benefit of this method in terms of mitigating attacks such as key-logging, man-in-the-middle, phishing or skimming and attacks through shoulder-surfing. Furthermore, the researcher in article [46] proposed codebook as a means of communicating the security string and conducted a user study, to find out the effect on usability. The result is encouraging as compared to similar existing method being used by EKO's.

3.3 METHODOLOGY AND APPROACH

A generic methodology discussed in reference [48] with objective of providing a generic approach for the design and development of secure mobile applications. Their approach treats a mobile application in a holistic way and structures it into four groups of modules: user interface modules, communication modules, security modules, and business logic modules. The researchers indicated that this approach other than making the design and development of secure mobile applications more efficient, flexible and expandable, it has the benefit of improving security of mobile application through data protection.

Similarly, the same researchers referenced in [48] proposed a model using Service Oriented Architecture (SOA), which is a way of organizing software, which has three main parts: a provider, a consumer, and a registry. Providers publish or announce their services on registries, where consumers find and then invoke them [49]. Their proposed model is called Secure SOA for mobile transaction [23]. Their model again is generic to be applied directly. It require many entities to be involved such as certificate authority, message dispatcher, registration agent, card manager and other. Beside this, It require end user device to have processing ca-

pability in order to get the security benefit.

To summarize, most of the researchers indicate that there exists security vulnerability on using SMS or USSD as a platform for mobile banking service. Authentication and confidentiality issues are the main vulnerability discussed by the researchers. However, most of these researchers, attempted to develop an end to end encryption that require client devices to have some processing capability for the client side application. But, solution may not be applicable for poor countries like Ethiopia with a lot of people using basic phone (Figure 2.3). Beside this, the one-time password proposed by some of authors as a solution for the authentication problem is not easy to use. It requires a code book or paper to be used during entering the password. Therefore, this study will fill these gabs and further enhance the security of mobile financial service platform through designing a secured yet usable mobile financial service model.

4

DESIGN AND PROTOTYPE IMPLEMENTATION

In this chapter, we discussed the proposed MFS framework which is designed to mitigate security limitations of the current USSD based platform.

4.1 PROPOSED FRAMEWORK FOR MOBILE FINANCIAL SERVICE

The proposed framework is designed based on SOA approach. This approach is selected for two main reasons. The first reason is SOA has been recommended by other similar works and archived a good result[23], [48]. The second reason is service-oriented computing is a modern approach to software design and provides a way to create a new architecture that reflects components' trends toward autonomy and heterogeneity [49]. In general, the MFS as a service is being provided by service providers such as banks. The role of MNO is to facilitate the communication process and act as an interface between service requesters (users) and service providers (such as banks).

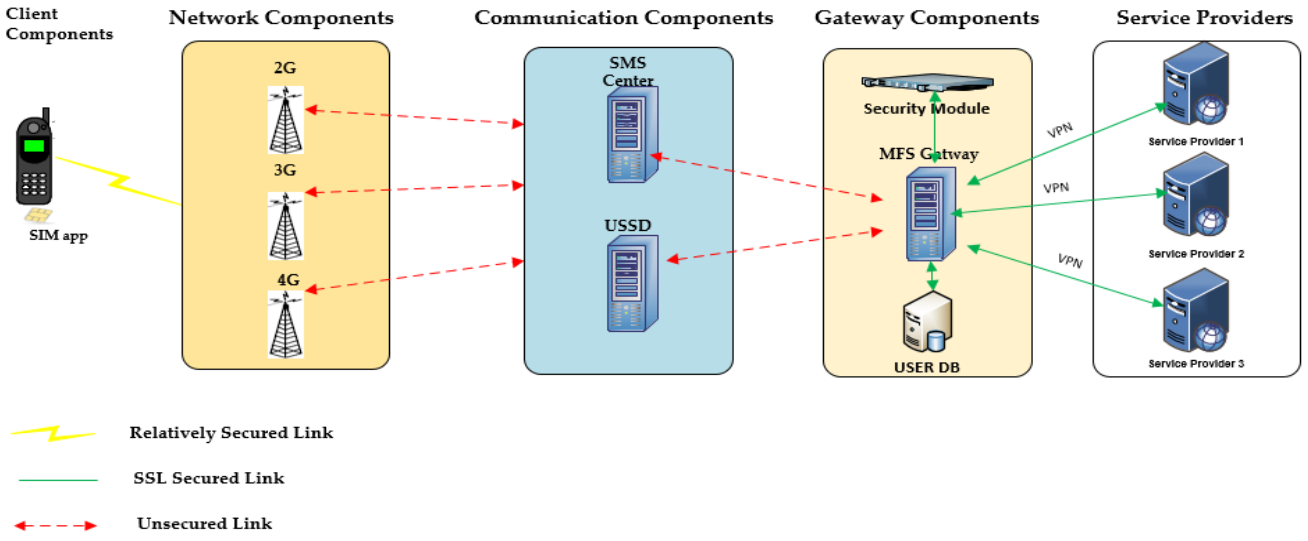

Figure 4.1: Components of proposed framework

4.1.1 *Components of Proposed Framework*

Figure 4.1 presents the main communication links between stakeholders such as users, banks or service providers, and MNO. The proposed framework incorporate SIM application and gateway components on top of existing model so as to provide the security services required for MFS. In general, the major components involved in this proposed framework are: client application, communication center, MFS Gateway and MFS Providers. Each of these components are discussed hereunder.

1. Client Application: As discussed in Section 2.6.1 the appropriate technology for Ethiopian market is to design application considering users with limited device. Hence the client application proposed in our method need to be developed on the SIM card. The client application is responsible for initiating service request based on menu either defined and installed on the SIM card or dynamically from the server using dynamic SIM toolkit (DSTK) technology.
2. Network Components: For mobile transactions, the main components on which the service is designed and developed is the mobile network which can be 2G, 3G or 4G. It is a link through which the client connect to the service provider.
3. Communication Components: This can be USSD or SMSC as both of them are text based communication channel and can be used as a bearer to transfer data from client application to MFS providers via the network components.
4. MFS Gateway Components: Operate as an interface between service requester in our case client application and service providers such as banks. It has additional components with in it such as security module which is responsible for cryptography and message digest operation as well as for key management. It also has a user database which contains a list of MFS users.
5. MFS Providers: Finally, the actual service will be defined in these components.

4.1.2 *Proposed Architecture*

The overall architecture of our proposed model is built on top of the existing GSM architecture. The model uses SIM based approach to implement end to end security of mobile financial transactions.

The proposed architecture is designed based on the generic framework shown on Figure 4.1. In this architecture, four main components are introduced as compared to the existing USSD based architecture. The newly added four components include: EIR, MFS gateway, MFS users' database and the SIM application.

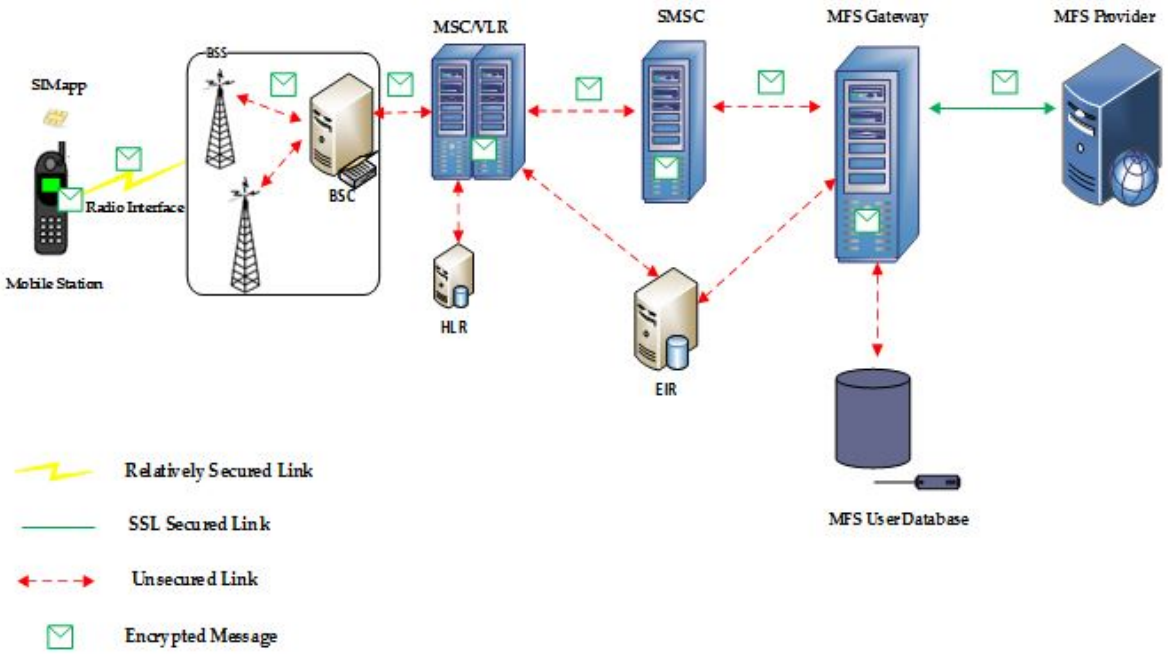

Figure 4.2: General architecture of the proposed framework

4.1.3 *Core Functions in the Proposed Framework*

4.1.3.1 *Registration*

This is the first activity whereby a mobile service user registers for MFS with service providers such as banks. The service provider, after completing registration on their side, communicate MNO all the necessary information such as Mobile Station International Subscriber Directory Number (MSISDN). The MNO registers

the user with their MSISDN and MFS provider number and install the STK based application on SIM card. The application is downloaded and installed using over-the-air (OTA) technique.

4.1.3.2 *Authentication and Authorization*

The mobile user authenticates itself first with the mobile network operator to verify if the user is registered for the MFS with the given service provider number. The MNO only forward the request if the customer is registered for the service. By doing so, the MNO avoid unnecessary session setup and reduce the possibility of DOS from MFS provider side. The bank also checks if the user is registered or not before allowing further activity by the user. Authorization process is based on the user's need. For operation that are not sensitive such as balance enquiry and air time charge to owner's number, a simple authentication is enough. On the other hand, if the operation is sensitive transaction such as cash withdrawal and bill payment a one time PIN code will be requested.

In our proposed model, the one time PIN code will be used rather than the PIN so as to further improve the security by avoiding attacks such as shoulder surfing. Like other similar works in reference [46], [47] the one time PIN code can be obtained by taking the character or digit available on the PIN code string by using the PIN as a position locater. For instance, on Figure 4.3 the PIN 3478 is used to locate the position of OTP code on the PIN code string. So, the first character or digit of OTP code is found on 3rd position, the second on 4th, the third on 7th and the fourth on 8th position of the PIN code string. However, in both study mentioned above, they only use digit, while in our proposed model characters are added on PIN code string to increase the challenge of getting the PIN through dictionary attack. Beside this, the communication method used in article [46] is codebook (listing the nonce in a paper form), which has usability problem as indicated by the researcher himself. On the other hand, communication method proposed in article [47] requires additional channel such as SMS to be used which may not be applicable for MFS as the main channel being used is on mobile device. In our case, we proposed the one time code to be displayed as a menu

header while users are requested to enter the PIN, which is better from usability aspect and does not require additional effort(reading codebook or SMS).

Locate the PIN →	0	1	2	**3**	**4**	5	6	**7**	8	**9**
PIN Code String →	1	2	h	**e**	**4**	5	9	**g**	8	**3**

Figure 4.3: PIN postion and One Time PIN code

4.1.3.3 *Data Transaction Operation*

In our proposed model, during data transaction two main actions take place from security perspective: encryption and message digestion.

In every transaction after the user gets the menu and enter his/her choice, sensitive information will be encrypted and MAC generated and send to MFS provider. The general steps presented as follows:

1. Client application on the SIM encrypt data and generate MAC. Here the encryption is using the triple DES key which exit in every SIM card. The MNO in our case ethio telecom assumed to have the list of keys together with their MSISDN. These keys are only known by the MNO and hence, the encrypted data will be first decrypted by the MNO using a security module.
2. The client application send the encrypted data via SMS to MFS Gateway.
3. On MFS gateway decrypt the data received and calculate MAC on the data.
4. Compare the MAC and if the same; encrypt the data using MFS provider's key.
5. Send the data to MFS provider via secured link such as VPN.

   This step is shown diagrammatically on Figure 4.4.

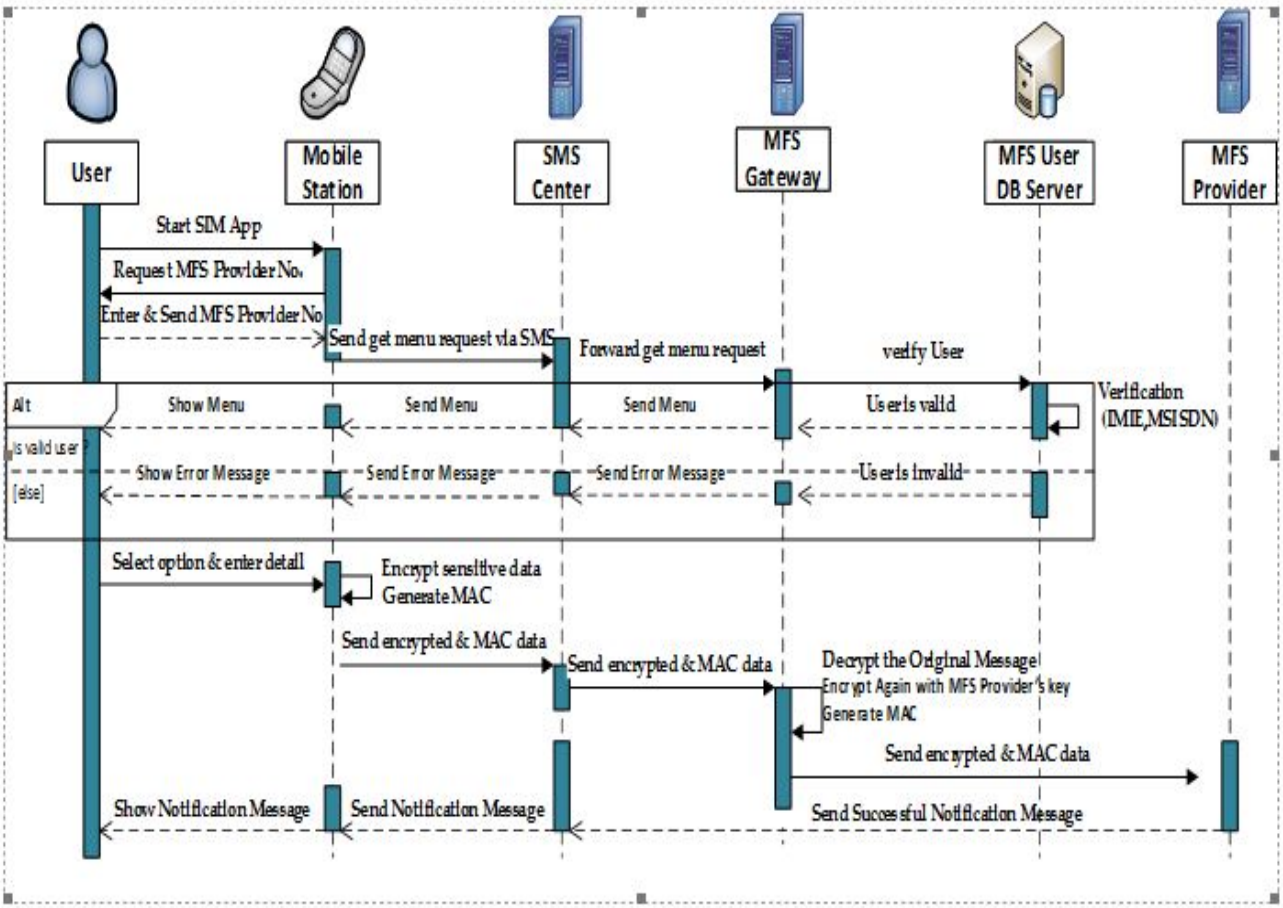

Figure 4.4: High level data transaction flow

4.2 PROTOTYPE DESIGN AND IMPLEMENTATION

Client server based prototype is designed and developed as a proof of work to show the security part. Accordingly, the client application which is SIM based solution is cable of encrypting the data using the key which resides in the SIM. In actual scenario the encrypted data will be forward via SMS while for simulation purpose simple http request–response used for the communication between the client and the server.

4.2.1 *User Interface Design*

The prototype application consists of two user interfaces one for USSD based and the other for SIM based approach. The USSD UI was designed and developed

based on a user interface adapted from CBE Birr of Commercial Bank of Ethiopia, while SIM based was developed following usability guidelines from literatures [14], [15]. As shown in Figure 4.5 from the left, the first UI is the main menu showing both UI link. The next UI from left next to main menu is the USSD based UI and the last is SIM UI. In general the SIM UI is designed to make the user interaction easy and user friendly. Rather than typing the choice as shown on the figure, on SIM UI the users can navigate on the list and select by touching the screen in the case of smart-phone or pressing a button in the case of basic and feature phones.

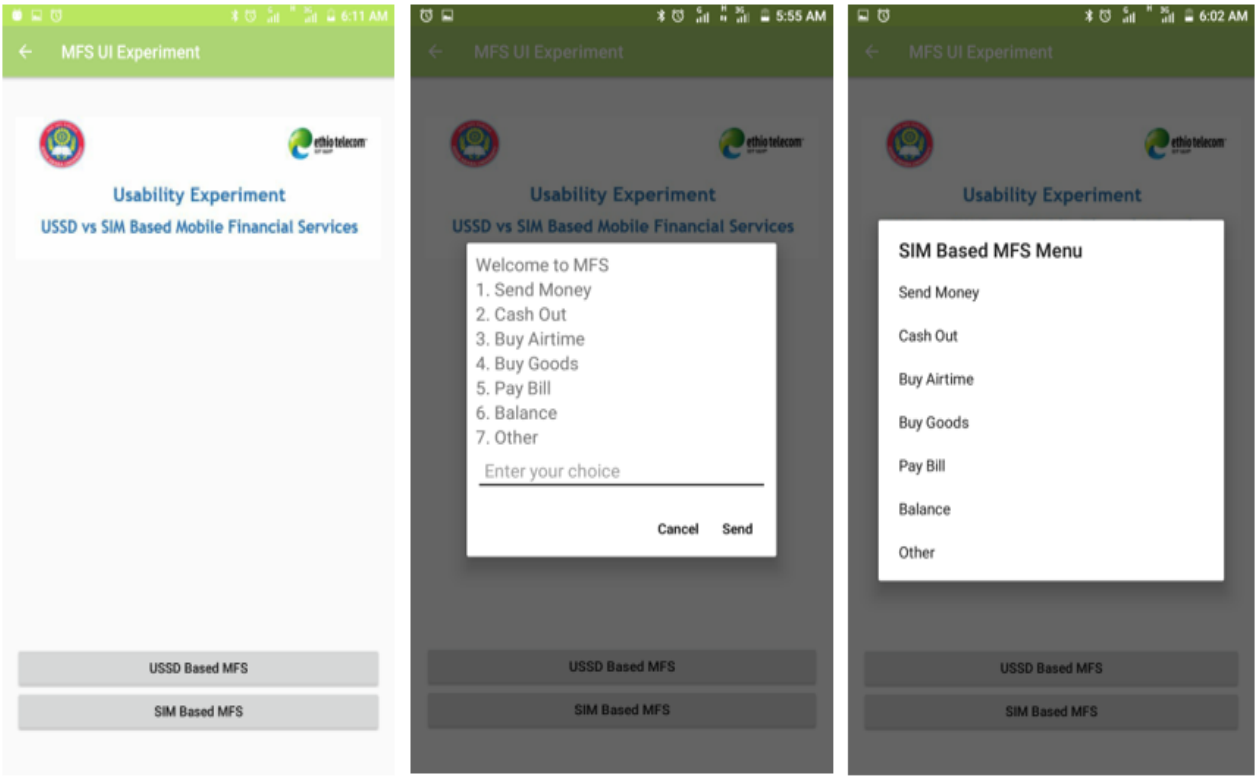

Figure 4.5: User interface designed for experiment

4.3 COMPARISON OF EXISTING AND PROPOSED MODEL

In this section discussion made on comparison of existing and proposed model in relation to usability and security design.

4.3.1 *Comparison Based on Security*

In general, there is no security mechanism in the case of existing model (USSD approach). While in the proposed model end to end security in-terms of data confidentiality and integrity can be achieved. Furthermore, the proposed model is better in-terms of authentication and availability from service provider side.

4.3.1.1 *Authentication*

Unlike the current USSD based model, that applies two factor authentication (MSISDN and PIN) , the proposed model uses multi-factor authentication by adding IMEI as part of increasing the security layer. Hence, in the proposed model, if the MFS gateway found that the user device is changed it will notify the case via SMS. By doing this at least it can reduce the risk.

On top of this, the PIN and MSISDN used for authentication in the existing model can easily be forged using vulnerabilities discussed in Section 2.8 such as through SIM cloning, fake base station and brute force attack. But, some service providers implemented automatic locking mechanism after three trials and this might help them to reduce brute force attack. This, however, most likely open door for another security attack called DOS, one scenario can be, a malicious user intentionally try wrong PIN number through sending many requests. The service provider locks account with three trails which ultimately create DOS both from customer and service provider side. Imagine when this happened for large number of customers. So, in our proposed model,through using one time PIN code without locking mechanism will avoid both of the problem listed above. Even for the brute force attack since our proposed one time code since it includes digits and characters which require relatively higher time to get the PIN than the current digit only PIN.

4.3.1.2 *Availability*

During discussion with IT VAS operation team one of the complaint raised from service providers is about unregistered users' request flooding their servers. This is because of the reason that the current USSD based model works in such a

way that MNO forward each and every request to service provider irrespective of whether the customer is registered for that service or not. Hence, this kind of repeated request either it can be intentionally or unintentionally may create flooding on the service provider's server and be a reason for DOS.

In the proposed model, by introducing the concept of holding the list of MFS users in the MNO database it will be possible to block the request from being forwarded to service provider's server and avoid unnecessary call setup from MNO side and DOS and unnecessary processing from service provider's side .

4.3.2 *Comparison Based on Usability*

In this paper, the usability parameters are mainly considered from UI design point of view since it is the main focusing area to improve usability[32]. Hence, the existing USSD based platform which uses text based UI is explored and found to be not user friendly as it does not follow most of the design guidelines discussed on Section 2.10.2.1. On the other hand, UI of the proposed model is designed following some of these guidelines so as to reduce the usability issues on USSD and improve efficiency by reducing user interaction.

Figure 4.6 shows some of the differences between SIM and USSD user interface. Accordingly, the first screen from the left labeled as 1 shows a SIM based application UI listing the menu and the possibility of allowing user to navigate by using the arrow buttons and selecting their choice simply pressing a button. Where as in the case of USSD based UI which is shown on screen labeled as 2, user need to enter their choice by typing text which violet the usability guidelines discussed on literature. Besides, in the case of smart phone as shown on the screen 3 the keypad displayed is not restricted to the input type. For instance, on screen 3 (USSD based UI) and on screen 4 (SIM based UI) user want to enter amount, on screen 3 the keypad shows both character and digit value while on screen 4 the keypad is limited to the type of data to be entered. By doing so, it will reduce error and improve time taken to input the information. Furthermore, screen 4 also shows SIM based UI searching facility from contacts rather than typing in the case of USSD

based UI. This is also one the requirements on the design guidelines indicated on Section 2.10.2.1.

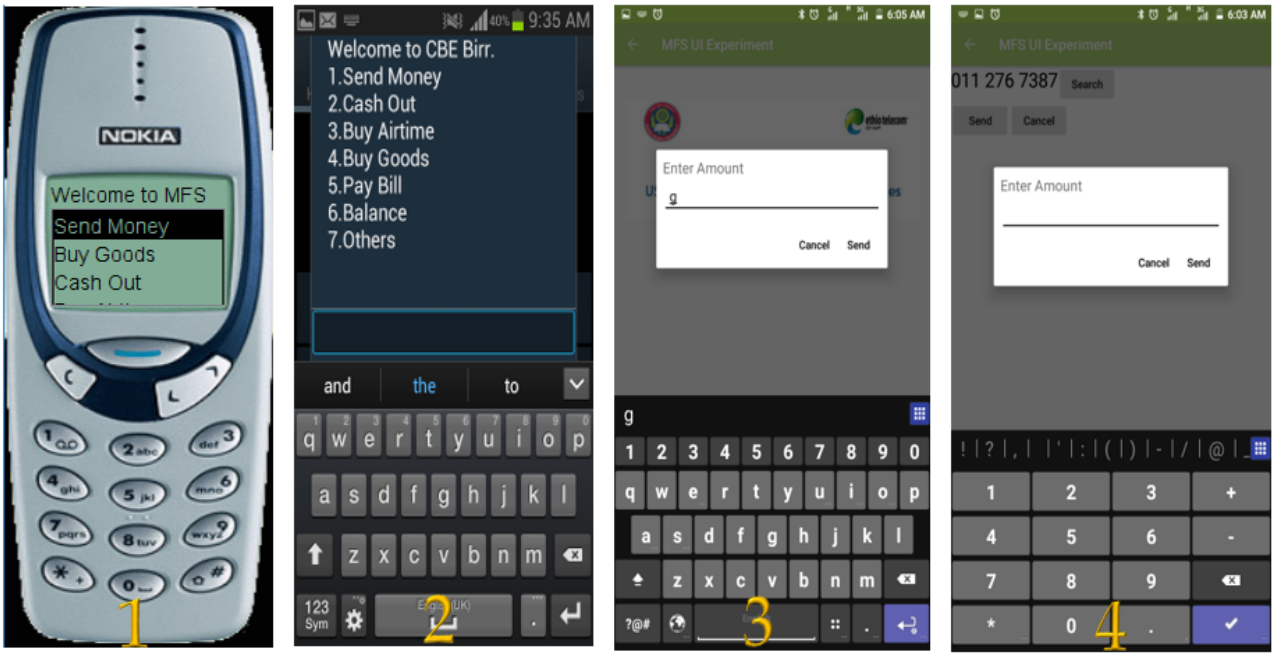

Figure 4.6: UI input method SIM and USSD based design

5

RESULT, DISCUSSION AND ANALYSIS

In this chapter, the results of the study are presented and discussed in detail followed by the security analysis of the proposed model with respect to the current model is made.

5.1 RESULTS

The results of the study are discussed in two parts. The first part is on security issues and the second part is on usability aspect.

5.1.1 *Security*

To evaluate the proposed model in terms of security, a prototype is designed and developed in a client-server based approach.The client application is a SIM based solution developed using Wireless Markup Language (WML). While the server side application, which is responsible for responding request from client, is developed using Java technology. In this prototype , security mechanisms such as cryptography and message digest were deployed to solve the problem of confidentiality and integrity respectively.

Figure 5.1 shows the server output after processing the client request for bill payment operation using mobile financial service. As shown on the figure a four digit PIN number **3024** is encrypted successfully on the client machine using application implemented on the SIM card. The figure also shows, the message digest result obtained by calculating Message Authentication Code (MAC) on transaction that need to be signed in this case **1120500**. Accordingly, both client and server generated similar MAC 0BE7B585.

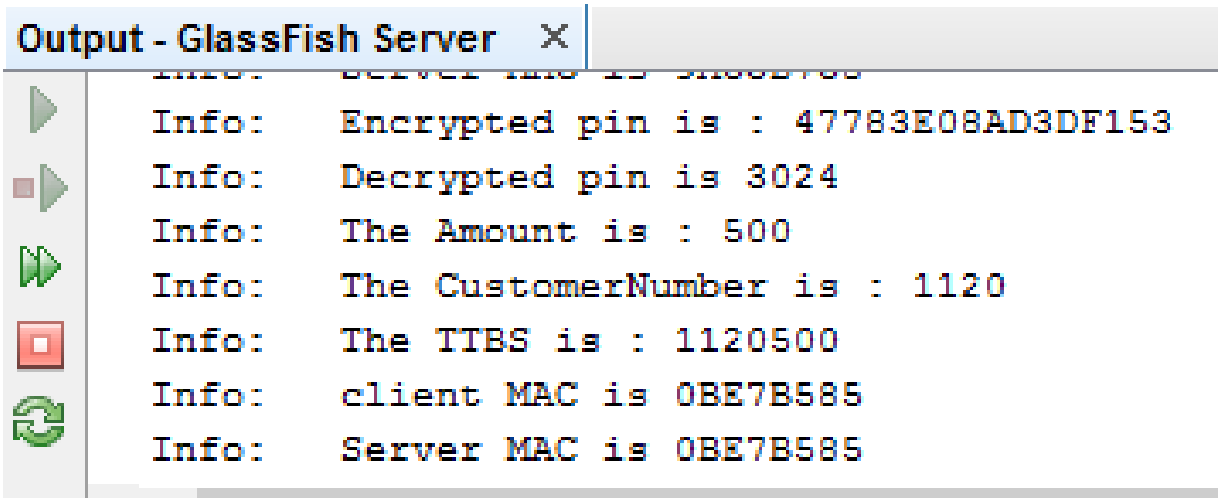

Figure 5.1: Server output showing prototype test result

Comparison of existing and proposed model in terms of security services have been made and the result is shown on Table 5.1. The existing USSD based MFS does not fulfill any of the requirement while the proposed model achieved two of the tree main security objectives i.e confidentiality and integrity. Though they are not the objectives of this research, availability and non repudiation can also be tackled partially using this model. Availability issues from MNO side is not within the scope of our work.

Table 5.1: Comparison of current (USSD Based) and proposed model

Criteria	**USSD Based**	**Proposed Framework**
Confidentiality	NO	YES
Integrity	NO	YES
Availability	NO	Partially Yes
Authentication	Two factor	Multi factor
Non repudiation	NO	Partially Yes

To verify the confidentiality of data communication on the proposed model a packet sniffer tool (wireshark) has been used. To capture the packet during data transfer from client application to the server both for USSD and SIM based approach. A simulation tool shown on Section A.6 has been used to simulate USSD operation between mobile device and USSD application. During the communica-

tion process packet captured shown on Figure 5.2 to see if sensitive information can be visible. Accordingly, the PIN forwarded to USSD application server from client is shown in plain text.

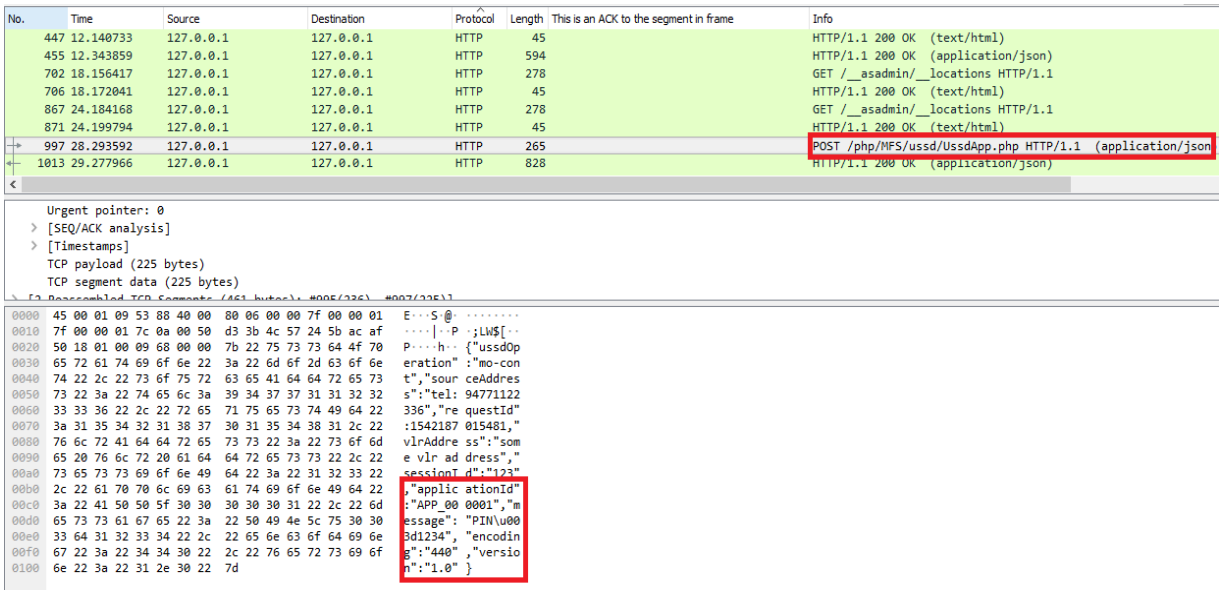

Figure 5.2: Packet sniffer output during USSD based communication

Similarly, packet captured during communication process using our proposed model shown on Figure 5.3 indicate that sensitive information such as PIN is encrypted and not visible in plain text as it does in USSD based model.

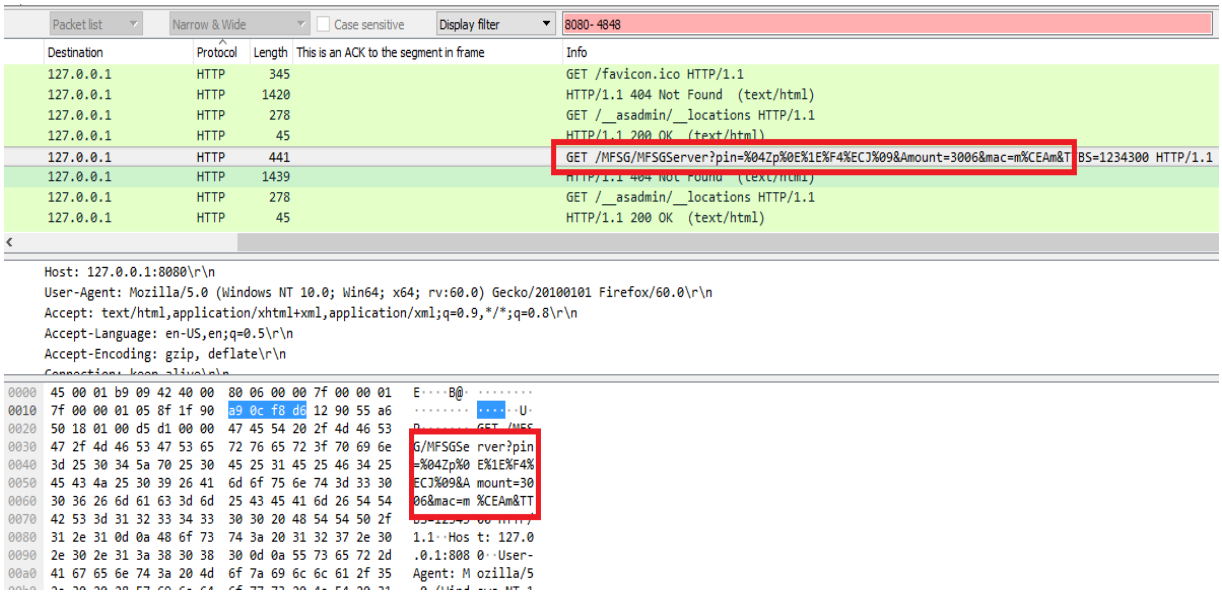

Figure 5.3: Packet sniffer output during SIM based communication

On the other hand, there is no mechanism defined on USSD based model to achieve integrity of the message being communicated. whereas in the case of SIM based approach, by applying MAC it is possible to mitigate the problem of data integrity on the current model. Figure 5.4 shows the effect of changing TTBS parameter value from 1234300 to 123430. As shown on the figure the MAC value sent from client was 6DCE416D and due to the change the server calculated MAC value and it become 2E6DAADD which is different from the original one. By doing this, data integrity verification can be achieved on the proposed model.

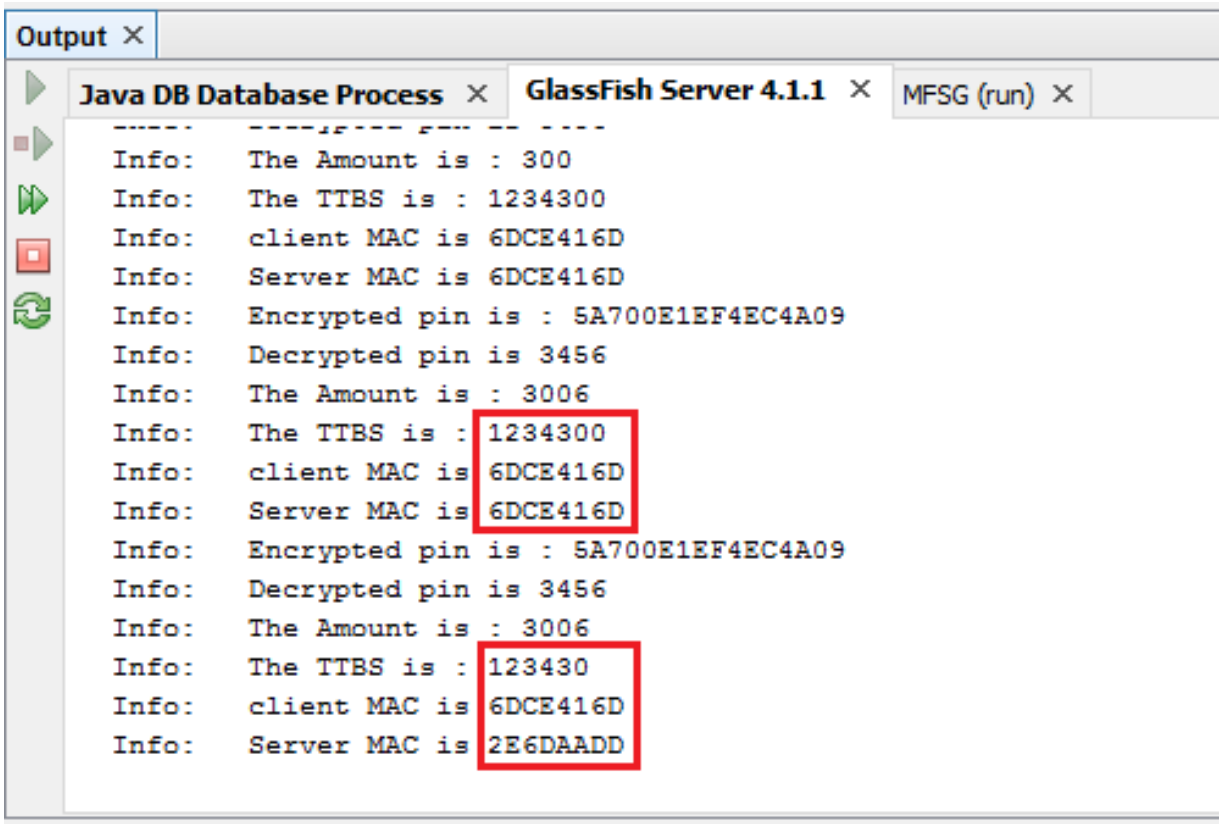

Figure 5.4: Proposed model message integrity verification

Furthermore, user study conducted to assess users' perception after using OTP on SIM based UI both in terms of difficulty to use and overall security perception. Table 5.2 indicates that mean value for users' perception on difficulty of using OTP and its implication in terms of overall security on USSD UI without applying additional securiry mechanism and SIM UI applying OTP code. The result shows that user level of perception highly increased for the SIM UI applying additional layer of security i.e OTP code as compared to the USSD UI.

Table 5.2: Mean value of Users' perception in relation to security (5 point Likert scale)

Difficulty of OTP	USSD Security	SIM app Security
3.14	2.89	4.68

5.1.2 *Usability*

Apart from security, the aim of the study was maintaining or improving usability advantage of existing USSD based approach. In this section, the details of user study experiment results are presented as follows.

5.1.2.1 *Participants' Profile*

From the total of 37 participants 68% of them are from ethio telecom and the remaining 32% are from Commercial Bank of Ethiopia. Most of the participants involved on the experiment are experienced (84% more than 5 years experience)and all of them are first degree or masters degree holders.

5.1.2.2 *Efficiency*

Unlike other usability elements, efficiency and error rate are measured objectively through recording timer and counting errors committed while participants were doing a given task.

Table 5.3 shows the descriptive result of the mean total times taken to complete send money operation using USSD UI and SIM UI. Participant took more time in the case of USSD UI than SIM UI both for simple and complex PIN.

A two way repeated measure ANOVA was performed to compare the effect of user interface on total completion time for a given task (send money operation). Participant were instructed to do the operation three time with different PINs (simple – complex). Accordingly, there was statistically significant difference on total time taken while using USSD based UI as compared to SIM based UI ($F(1,36)= 53.546, p= 0.0001$).

Table 5.3: Mean total time taken (sec) to complete using USSD and UI with simple and complex PIN

	Mean	**Std. Deviation**	**N**
USSD_Simple_PIN	39.78	4.008	37
USSD_Complex_PIN	35.84	4.586	37
SIM_Simple_PIN	31.84	4.925	37
SIM_Complex_PIN	32.46	4.141	37

5.1.2.3 *Error Rate*

Another usability characteristics evaluated in the experiment was the number of errors committed while performing send money operation. Accordingly, no error reported for USSD UI and also on average nearly zero error have been recorded for SIM UI.

5.1.2.4 *Other Usability Elements*

The result as depicted on Table 5.4 users' perception and preference in terms of other usability elements such as learnability, satisfaction and ease of use is higher for USSD UI than SIM UI.

Table 5.4: Comparison of USSD UI and SIM UI (mean value in 5 point likert scale) on usability elements

	Learnability	**Satisfaction**	**Ease of Use**
USSD UI	4.35	3.90	4.21
SIM Based UI	3.78	3.81	3.76

Another interesting result shown on Figure 5.5 is USSD based UI significantly took higher time to complete than SIM UI while using simple PIN. The mean value decrease moderately for USSD and increase slightly for SIM based UI while using complex PIN.

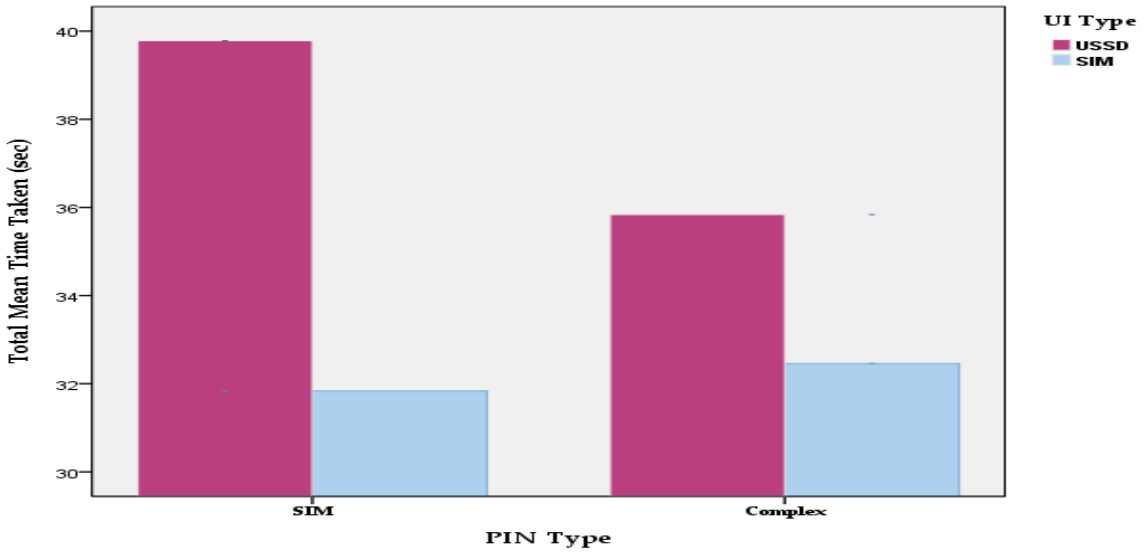

Figure 5.5: Total mean time taken to complete a given task USSD vs SIM based UI

On the other hand, it is not surprising to see significantly higher mean authentication time for SIM based UI while using complex PIN as compared to USSD. This can be due to the reason that OTP code is incorporated on SIM based UI design (Figure 5.6).

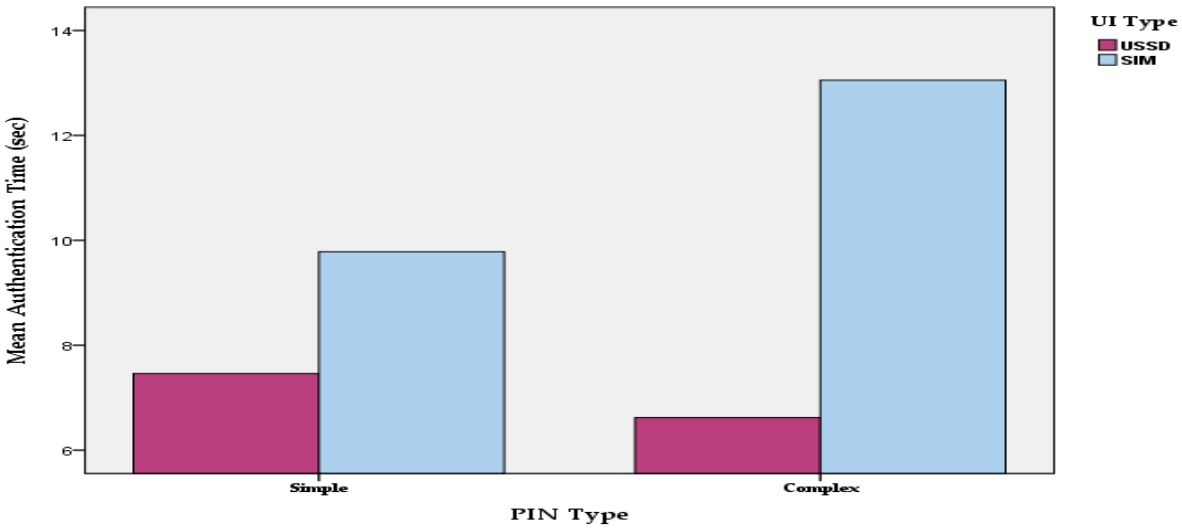

Figure 5.6: Mean authentication time USSD vs SIM based UI

5.1.2.5 *Perception*

User study result obtained with regard to security perception was a mean value of 2.89 for USSD and 4.67 for the proposed SIM approach on five point likert scale. Due to the OTP code feature proposed on our model, the user's perception for

security is better for SIM based approach than USSD.

On the other hand, the overall perception of participants preference was SIM based as compared to USSD. In terms of percentage 94.6% of participant choose SIM based and the remaining 5.4% prefer the current USSSD.

Overall,the results from the user study indicate that the proposed model is efficient in terms of total time taken to complete a given task. Although, the proposed model took more time during authentication which happened due to the one time PIN code proposed it reduce the total time taken through making improvement on other elements of the UI.

5.2 SECURITY ANALYSIS OF PROPOSED MODEL

Analysis have been made on the end to end security of the proposed framework in terms of criteria set out by international organization such as ITU, NIST and ISO with regard to confidentiality, integrity and availability.

In general, these criteria include confidentiality, integrity, availability non-repudiation, and authentication services. Brief description is given below to show how these services are addressed in our model.

5.2.1 *Confidentiality*

End to end encryption applied on every sensitive data transaction from SIM card to MFS providers. Symmetric key ciphers which is available on the SIM are used to encrypt message contents so as to ensure data confidentiality. Since the SIM card encryption keys are only known by MNO the encryption process is performed in two stages. The first one, between the SIM card and MFS gateway the second one between MFS gateway and service providers using a shared key.

5.2.2 *Integrity*

In our model message digest technique (MAC) is proposed to ensure message integrity where hashes of message contents are calculated at ends and then compared. the difference indicate integrity issue. Unlike other message digest technique, MAC uses encryption key to make it difficult for anyone with out having the key to generate similar value.

5.2.3 *Authentication*

The proposed model uses multi-factor authentication unlike that of the existing system which uses two factor. User is first authenticated to the system using a MSISDN and IMEI. If there is a change of device from what has been registered on the MFS user database, notification message will be sent to the user as part of the security mechanism to protect or reduce the attack if any through masquerading. If there is no issue with MNO verification, PIN will be requested for sensitive transaction such as cash withdrawal or payment. To further increase the security layer, OTP code will be used instead of the PIN itself to reduce attack such as shoulder surfing.

In general, the proposed model uses a multifactor authentication (MSISDN, IMEI and PIN) unlike the existing two factor authentication (MSISDN and PIN)

5.2.4 *Availability*

As indicated on the scope of the study this security service is not covered on our model. But we consider the problem of availability from service providers' side due to getting wrong request from unregistered user. Through registering MFS users it can be possible to avoid unnecessary call setup and DOS from service provider side.

5.2.5 *Non-repudiation*

We did not fully mitigate the problem of non-repudiation in our model. Partially, the OTP code and the symmetric key used which reside on tamper resistance SIM during the communication process can be used as a parameter though are not fully effective in resolve the problem of non-repudiation. Since only this key can encrypt messages that will be successfully decrypted by the server, neither of the parties can deny its involvement in any transaction.

6

CONCLUSION AND FUTURE WORK

6.1 CONCLUSION

In this study different MFS technologies are explored considering the existing situation of ethio telecom in terms of customers' phone type, users' literacy level, technology used, usability, security requirement and the like. Accordingly, it is concluded that most of ethio telecom customers' device are resource limited, most unbanked citizen have low literacy level, low adoption rate due to security and usability perception. Therefore, through exploring and analyzing technology options in line with these existing situations in Ethiopia we proposed SIM based solution for mobile financial services.

Based on findings from literatures, the current USSD based model, known to have many vulnerabilities. This vulnerabilities can be on mobile station, air interface, operator internal network or the platform itself. In general, the existing USSD based MFS model does not have a security mechanism by itself rather it relies on the GSM security which itself has known vulnerabilities. Hence, Its level of security (based on ITU recommendation) fall under level 1 which is too low to be used for financial transaction that require at least level 3 for better security [40]. To overcome this problem and improve the security level from level one to level three, we proposed a security mechanisms to be implemented on SIM based approach. Using this approach it is possible to implement end to end security through encryption techniques on the SIM card via STK technology. Moreover, since the solution is designed and developed in application form, there is flexibility in terms of making UI better in terms of usability through applying best practices and guidelines.

The newly proposed model is more secure in terms confidentiality and integrity through applying a well known encryption algorithm and MAC on sensitive information. Furthermore, the authentication mechanism used in the current model is

simple though it is a two factor. The pin can be guessed using brute force attack or can be vulnerable for DOS attack if the service provider lock the PIN after three wrong trail. Besides, MSISDN can be faked using SIM clone or fake base station. In our model we proposed a flavor of multi-factor authentication by incorporating IMEI on top of the existing two factor model used by the current platform. Beside this, the one time PIN code proposed in our model improved the security and users' perception on security. In addition to these, the proposed model mitigate the vulnerability with regard to session creation for illegitimate request through applying a simple solution of registering MFS users in MNO system.

In general, based on the analysis we made following the evaluation of the proposed model from security point of view, we found encouraging results. In most of the security requirements recommended by international standards such as authenticity, confidentiality, non-repudiation, message integrity, and availability the proposed model is better than the existing USSD model.

Furthermore, in this study we developed a prototype UI and conducted user study in order to evaluate usability of both existing and proposed model in terms of user interface. Based on the results, USSD based UI took more time as compared to the proposed SIM based application UI. On the other hand, participants preferred the existing USSD UI in terms of some of the other usability parameters such as satisfaction, ease of use and learnability. However, the overall preference is in favor of SIM based UI which is 94.6% of the participant preferred our proposed model and most of them stating the security improvement as a reason.

6.2 FUTURE WORK

In terms of security, the main issue that need further checking is the key management and distribution part. In our proposed model, we used the existing triple DES key, which is available on the SIM, for the encryption and MAC generation process. Many researches have been made which suggest the key management and distribution issues in mobile applications security but the applicability of their technique in Ethiopian context need to be analyzed and evaluated in terms of re-

source requirement and performance. In addition to this, if there is a possibility to get SIM manipulation tool such as SIM reader, further feasibility checking of the proposed solution and evaluation of more advanced security solution such as PKI and comparing it with our symmetric key based approach can be area for future study. Furthermore, security element such as non-repudiation need further study as it is critical element in the case of mobile banking since either service requester or service provider can deny their involvement on the transaction.

With regards to usability, the user study undertaken on this research only involves experts opinion and feedback through experiment and questionnaire. More usability issues can be identified by involving the ultimate users during the design process and through analyzing user experience on filed. By following an iterative approach to come up with a better user interface which most likely improve adoption rate for mobile financial service.

BIBLIOGRAPHY

[1] ethio Telecom. (2018). home page ethiotelecom, [Online]. Available: http://www.ethiotelecom.et.

[2] S. M. Arif, "Ethiopian bankers perception of electronic banking in ethiopia–a case of adama city," *International Journal of Scientific and Research Publications*, vol. 4, no. 9, 2014.

[3] A. Demirguc-Kunt, L. Klapper, D. Singer, S. Ansar, and J. Hess, *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*. The World Bank, 2018.

[4] N. B. of Ethiopia, *National Bank of Ethiopia Quarterly Bulletin*, 1. National Bank of Ethiopia, 2018, vol. 34.

[5] Z. Ahmed, A. Kader, H. U. Rashid, and M. Nurunnabi, "User perception of mobile banking adoption: An integrated ttf-utaut model," *Journal of Internet Banking and Commerce*, vol. 22, no. 3, pp. 1–19, 2017.

[6] R. Priya, A. Vikas Gandhi, and A. Shaikh, "Mobile banking: Consumer perception towards adoption," vol. 25, pp. 00–00, Jan. 2018.

[7] F. O. Bankole, O. Bankole, and I. Brown, "Mobile banking adoption in nigeria," vol. 47, Jul. 2011.

[8] A. G. Bultum, "Factors affecting adoption of electronic banking system in ethiopian banking industry," *Journal of Management Information System and E-commerce*, vol. 1, no. 1, pp. 1–17, 2014.

[9] A. DESALGEN, "Factors affecting usage of mobile banking service in commercial bank of ethiopia," Master's thesis, St. Mary's University, 2017.

[10] A. B. Mtaho, "Improving mobile money security with two-factor authentication," *International Journal of Computer Applications*, vol. 109, no. 7, 2015.

[11] S. Desai, "Mitigating security risks in ussd-based mo-bile payment applications," 2011.

[12] K. K. Lakshmi, H. Gupta, and J. Ranjan, "Ussdarchitecture analysis, security threats, issues and enhancements," in *Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS), 2017 International Conference on*, IEEE, 2017, pp. 798–802.

[13] B. W. Nyamtiga, A. Sam, and L. S. Laizer, "Enhanced security model for mobile banking systems in tanzania," *Intl. Jour. Tech. Enhancements and Emerging Engineering Research*, vol. 1, no. 4, pp. 4–20, 2013.

[14] N. Jailani, Z. Abdullah, M. A. Bakar, and H. R. Haron, "Usability guidelines for developing mobile application in the construction industry," in *Electrical Engineering and Informatics (ICEEI), 2015 International Conference on*, IEEE, 2015, pp. 411–416.

[15] A. S. Badashian, M. Mahdavi, A. Pourshirmohammadi, *et al.*, "Fundamental usability guidelines for user interface design," in *Computational Sciences and Its Applications, 2008. ICCSA'08. International Conference on*, IEEE, 2008, pp. 106–113.

[16] GSMA, "The mobile economy 2018," GSM Association, research rep., 2018. [Online]. Available: https://www.gsma.com/mobileeconomy/.

[17] A. C. Ltd. (Aug. 11, 2018). Gsm network architecture. I. Poole, Ed., [Online]. Available: https://www.radio-electronics.com/info/cellulartelecomms/gsm_technical/gsm_architecture.php.

[18] G. T. Krugel, "Mobile banking technology options," *FinMark Trust*, 2007.

[19] M. Toorani and A Beheshti, "Ssms-a secure sms messaging protocol for the m-payment systems," in *Computers and Communications, 2008. ISCC 2008. IEEE Symposium on*, IEEE, 2008, pp. 700–705.

[20] F. Schwenke, "Access channels for mobile banking applications: A comparative study based on characteristics," Master's thesis, Cape Peninsula University of Technology, 2009.

[21] L. Perlman, "Technology evolution and innovation in digital financial services (dfs)," International Telecommunication Union, Geneva, Tech. Rep., 2017.

[22] G. Ramesh and F. Abadi, "A security protocol for mobile-banking and payment using sms and ussd in ethiopia," Jun. 2016.

[23] F. Zhang, S. Muftic, and G. Schmöelzer, "Secure service-oriented architecture for mobile transactions," in *Internet Security (WorldCIS), 2011 World Congress on*, IEEE, 2011, pp. 133–138.

[24] J Bezuidenhoudt and D. Porteous, "Managing the risk of mobile banking technologies," *Bankable Frontier Associates, FinMark Trust*, 2008.

[25] M. Nieles, K. Dempsey, and V. Y. Pillitteri, "An introduction to information security," *NIST Special Publication*, vol. 800, p. 12, 2017.

[26] M. Rouse, M Haughn, and S Gibilisco, *Confidentiality, integrity, and availability (cia triad)*, 2014.

[27] B. A. Forouzan and F. Mosharraf, *Foundations of computer science*. Cengage Learning EMEA, 2008.

[28] B. A. Forouzan and D. Mukhopadhyay, *Cryptography and network security (Sie)*. McGraw-Hill Education, 2011.

[29] IBM. (Aug. 28, 2018). Security concepts and mechanisms, [Online]. Available: https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009730_.htm.

[30] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, vol. 2, no. 1, p. 1, 2018.

[31] M. M. Althobaiti and P. Mayhew, "Security and usability of authenticating process of online banking: User experience study," in *Security Technology (ICCST), 2014 International Carnahan Conference on*, IEEE, 2014, pp. 1–6.

[32] J. Nielsen, *Usability 101: Introduction to usability*, 2012.

[33] I. 9241-11, "Ergonomics of human-system interaction part 11: Usability: Definitions and concepts," *International Organization for Standardization (ISO)*, 2018.

[34] D. Zhang and B. Adipat, "Challenges, methodologies, and issues in the usability testing of mobile applications," *International journal of human-computer interaction*, vol. 18, no. 3, pp. 293–308, 2005.

[35] K. H. Moe, B. Dwolatzky, and R. Olst, "Designing a usable mobile application for field data collection," in *AFRICON, 2004. 7th AFRICON Conference in Africa*, IEEE, vol. 2, 2004, pp. 1187–1192.

[36] N. Anwar, I. Riadi, and A. Luthfi, "Forensic sim card cloning using authentication algorithm," *International Journal of Electronics and Information Engineering*, vol. 4, no. 2, pp. 71–81, 2016.

[37] T. Engel, "Ss7: Locate. track. manipulate," in *Talk at 31st Chaos Communication Congress*, 2014.

[38] P. J. H. Kruger, "Cellphone banking at the bottom of the pyramid," Master's thesis, Stellenbosch: Stellenbosch University, 2012.

[39] M. B. Association. (May 22, 2018). Mobile banking overview, [Online]. Available: https://www.mmaglobal.com/files/mbankingoverview.pdf.

[40] ITU-T, "Security requirements for mobile remote financial transactions in next generation networks," International Telecommunication Union, Geneva, Recommendation Y.2740, 2011.

[41] B. Belete, "Conceptual security framework for mobile banking key authentication and message exchange protocols: Case of ethiopian banks," Master's thesis, St. Mary's University, 2017.

[42] A. Emmanuel and B. Jacobs, "Mobile banking in developing countries: Secure framework for delivery of sms-banking services," *Radboud University Nijmegan, The Netherland*, 2007.

[43] Q. Tang, J. Zou, C. Fan, and X. Zhang, "A mobile identity authentication scheme of e-commerce based on java-sim card," in *Information Networking and Automation (ICINA), 2010 International Conference on*, IEEE, vol. 2, 2010, pp. V2–114.

[44] J. Breier and A. Pomothy, "Qualified electronic signature via sim card using javacard 3 connected edition platform," in *Availability, Reliability and Security (ARES), 2014 Ninth International Conference on*, IEEE, 2014, pp. 349–355.

[45] M. K. Chong, "Usable authentication for mobile banking," Master's thesis, University of Cape Town, 2009.

[46] S. Panjwani and E. Cutrell, "Usably secure, low-cost authentication for mobile banking," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, ACM, 2010, p. 4.

[47] S. A. Systems, "Pinsafe multifactor authentication solution," Jul. 27, 2018. [Online]. Available: https://www.infopoint-security.de/open_downloads/2009/Swivel_PINsafe_Multifactor_Authentication_0309.pdf.

[48] F. Zhang, I. Kounelis, and S. Muftic, "Generic, secure and modular (gsm) methodology for design and implementation of secure mobile applications," in *6th International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2012; Rome; Italy; 19 August 2012 through 24 August 2012*, International Academy, Research and Industry Association (IARIA), 2012, pp. 1–6.

[49] M. N. Huhns and M. P. Singh, "Service-oriented computing: Key concepts and principles," *IEEE Internet computing*, vol. 9, no. 1, pp. 75–81, 2005.

APPENDIX TEST

A.1 SERVER SIDE JAVA CODE TO SIMULATE MFS GATEWAY

```
import java.io.IOException;
import javax.servlet.ServletException;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;
import java.util.*;

/**
*
* @author Asrar.Mohammed
* October 19, 2018
*/
public class MFSGServer extends HttpServlet {

private static String key = "1133557799bbddffffddbb99775533111133557799bbddff
    ";
private final byte[] iv = null;
@Override
public void init() throws ServletException { }

public void doGet(HttpServletRequest request, HttpServletResponse
response) throws ServletException, IOException {
getRequest(request,response);
}
public void doPost(HttpServletRequest request, HttpServletResponse
response) throws ServletException, IOException {
```

```
getRequest(request,response);
}
public void getRequest(HttpServletRequest request, HttpServletResponse
    response) throws ServletException, IOException {

Enumeration e = request.getParameterNames();
if (request.getQueryString().contains("pin") )
{
while (e.hasMoreElements()) {
String ss= (String)e.nextElement();
try {
if (!ss.equalsIgnoreCase("pin")) {
if (!ss.equalsIgnoreCase("mac")) {
System.out.println("The "+ss+" is : " + request.getParameter(ss));
}
else {
String mac = bytesToHex(request.getParameter(ss).getBytes("ISO-8859-1"));
}
}
else {
String encryptedPin = bytesToHex(request.getParameter(ss).getBytes("ISO
    -8859-1"));
encryptedPin = encryptedPin.substring(2,encryptedPin.length());
System.out.println("Encrypted "+ss+" is : " + encryptedPin );
cryptography cr = new cryptography();
String decodedmsg = cr.decrypt(encryptedPin, key);
System.out.println( "Decrypted pin is " + decodedmsg);
}
}
catch(Exception ee)
{
throw new IOException(ee.getMessage());
}
}
```

```
try {
byte[] cData = ( request.getParameter("TTBS")).getBytes("ISO-8859-1");
String cMAC = bytesToHex(request.getParameter("mac").getBytes("ISO-8859-1"));
byte[] keys = hexToByte(key);
cryptography cr = new cryptography();
byte[] sMAC = cr.verifyMAC(keys,cData);
String bsMAC = bytesToHex(sMAC);
System.out.println("client MAC is " + cMAC);
System.out.println("Server MAC is " + bsMAC);
System.out.println();
}
catch(Exception ee)
{
throw new IOException(ee.getMessage());
}
}
this.getServletContext().getRequestDispatcher("/client.wml").forward(request,
    response);
}
public static byte[] hexToByte(String str) {
int strlength = str.length();
byte[] bytArr = new byte[strlength / 2];
for (int i = 0; i < strlength; i += 2) {
bytArr[i / 2] = (byte) ((Character.digit(str.charAt(i), 16) << 4)+ Character.
    digit(str.charAt(i+1), 16));
}
return bytArr;
}
private final static char[] hexnum = "0123456789ABCDEF".toCharArray();
public static String bytesToHex(byte[] bytes)
{
char[] hexchar = new char[bytes.length * 2];
for ( int i = 0; i < bytes.length; i++ )
{
```

```
int j = bytes[i] & 0xFF;
hexchar[i * 2] = hexnum[j >>> 4];
hexchar[i * 2 + 1] = hexnum[j & 0x0F];
}
return new String(hexchar);
}
public void destroy() { }
}

================================================================================
import java.security.Key;
import java.util.Arrays;
import javax.crypto.Cipher;
import javax.crypto.SecretKey;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.SecretKeySpec;
/**
*
* @author Asrar.Mohammed
*/
public class cryptography {

private IvParameterSpec iv = new IvParameterSpec(new byte[] { 0, 0, 0, 0, 0,
    0, 0, 0 });
public static void main(String[] args) throws Exception
{
}
private Key key = null;
public  String decrypt(String encdata, String secretKey)
{
try
{
byte[] byteencData = hexToByte(encdata);
byte[] keyData = hexToByte(secretKey);
```

```
key = new SecretKeySpec(keyData, "DESede");
Cipher cipher = Cipher.getInstance("DESede/CBC/NOPadding");
cipher.init(Cipher.DECRYPT_MODE, key,iv);
byte[] decData = cipher.doFinal(byteencData);
String plainData = new String(decData, "utf-8");
return plainData;
}
catch(Exception ex) {
return ex.getMessage();
}
}
private Key key2 = null;
public String encrypt(String encdata, String secretKey)
{
try {
byte[] pdata = hexToByte(encdata);
byte[] encdata2 = Addpadding(pdata);
byte[] keyData = hexToByte(secretKey);
System.out.println("encryption key is " + keyData);
key2 = new SecretKeySpec(keyData, "DESede");
Cipher cipher = Cipher.getInstance("DESede/CBC/NOPadding");
cipher.init(Cipher.ENCRYPT_MODE, key2,iv);
byte[] decData = cipher.doFinal(encdata2);
String plainData = new String(decData, "utf-8");
return plainData;
}
catch(Exception ex) {
return ex.getMessage();
}
}
public static byte[] Addpadding(byte[] data) {

System.arraycopy(data, 0, new byte[] { (byte) 0x10 }, 0, 0);
int blockSize = 16;
```

```
if (data.length % blockSize == 0)
return data;
byte[] paddedData = Arrays.copyOf(data, data.length + blockSize - (data.
    length % blockSize));
return paddedData;
}
public byte[] verifyMAC(byte[] key, byte[] data) {
byte[] block;
byte[] edata;
byte[] key1 = Arrays.copyOf(key, 8);
byte[] key2 = Arrays.copyOfRange(key, 8, 16);
byte[] pdata = Addpadding(data);
try
{
SecretKey ka = new SecretKeySpec(key1, "DES");
Cipher cipherA = Cipher.getInstance("DES/CBC/NoPadding");
cipherA.init(Cipher.ENCRYPT_MODE, ka,iv);
SecretKey kb = new SecretKeySpec(key2, "DES");
Cipher cipherB = Cipher.getInstance("DES/CBC/NoPadding");
cipherB.init(Cipher.DECRYPT_MODE, kb,iv);
edata = cipherA.doFinal(pdata);
edata = cipherB.doFinal(edata);
edata = cipherA.doFinal(edata);
block = Arrays.copyOf(edata,  4);
}
catch (Exception e)
{
e.printStackTrace();
return null;
}
return block;
}
private final static char[] hexnum = "0123456789ABCDEF".toCharArray();
public static String bytesToHex(byte[] bytes)
```

```
{
char[] hexchar = new char[bytes.length * 2];
for ( int i = 0; i < bytes.length; i++ )
{
int j = bytes[i] & 0xFF;
hexchar[i * 2] = hexnum[j >>> 4];
hexchar[i * 2 + 1] = hexnum[j & 0x0F];
}
return new String(hexchar);
}
public static byte[] hexToByte(String str) {
int strlength = str.length();
byte[] datainByte = new byte[strlength / 2];
for (int i = 0; i < strlength; i += 2) {
datainByte[i / 2] = (byte) ((Character.digit(str.charAt(i), 16) << 4)+
    Character.digit(str.charAt(i+1), 16));
}
return datainByte;
}
}
```

A.2 CLIENT SIDE CODE USING WIRELESS MARKUP LANGUAGE

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<wml xmlns="http://www.smarttrust.com/WIG-WML/5.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.smarttrust.com/WIG-WML/5.0
http://www.smarttrust.com/xsd/wigwml-5.0.xsd">
<card id="START">
<p>
<select  title="Welcome to MFS">
<option onpick="#SM">Send Money</option>
<option onpick="#BG">Buy Goods</option>
```

```
<option onpick="#CO">Cash Out</option>
<option onpick="#SM">Buy Airtime</option>
<option onpick="#PB">Pay Bill</option>
<option onpick="#OT">Other</option>
</select>
</p>
</card>
<card id="SM">
<p>
<input title="Mobile Number:" name="mnum" format="*N"/>
<input title="Amount:" name="amt" format="*N"/>
<setvar name="TTBS" value="$(amt)$(mnum)" class="Binary" />
<setvar name="KeyID" value="\x03" class="Binary"/>
<setvar name="OPTS" value="\x00" class="Binary"/>
<setvar name="CES" value="S" class="Binary"/>
<plugin name="*DS" params="$(KeyID)$(OPTS)$(CES)$(TTBS)" destvar="MAC"/>
<input title="Enter  Pin:" name="cpin" format="*N"/>
<plugin name="ENCR" params="\x01$(cpin)" destvar="CipherText"/>
<do type="accept">
<go
href="http://localhost:8080/MFSG/MFSGServer?pin=$(CipherText)&amp;Amount=$(
    amt)&amp;MobileNumber=$(mnum)&amp;mac=$(MAC)&amp;TTBS=$(TTBS)"/>
</do>
</p>
</card>
<card id="BG">
<p>
<input title="Customer  Number:" name="cnum" format="*N"/>
<input title="Amount:" name="amt" format="*N"/>
<setvar name="TTBS" value="$(cnum)$(amt)" class="Binary" />
<plugin name="*SIGN" params="\x03$(TTBS)" destvar="MAC"/>
<input title="Enter  Pin:" name="cpin" format="*N"/>
<plugin name="ENCR" params="\x01$(cpin)" destvar="CipherText"/>
<do type="accept">
```

```
<go
href="http://localhost:8080/MFSG/MFSGServer?pin=$(CipherText)&amp;Amount=$(
    amt)&amp;mac=$(MAC)&amp;TTBS=$(TTBS)"/>
</do>
</p>
</card>
<card id="PB">
<p>
<input title="Customer  Number:" name="cnum" format="*N"/>
<input title="Amount:" name="amt" format="*N"/>
<setvar name="TTBS" value="$(cnum)$(amt)" class="Binary" />
<plugin name="*SIGN" params="\x03$(TTBS)" destvar="MAC"/>
<input title="Enter  Pin:" name="cpin" format="*N"/>
<plugin name="ENCR" params="\x01$(cpin)" destvar="CipherText"/>
<do type="accept">
<go
href="http://localhost:8080/MFSG/MFSGServer?pin=$(CipherText)&amp;Amount=$(
    amt)&amp;mac=$(MAC)&amp;TTBS=$(TTBS)"/>
</do>
</p>
</card>
<card id="CO">
<p>
<input title="Mobile Number:" name="mnum" format="*N"/>
<input title="Amount:" name="amt" format="*N"/>
<setvar name="TTBS" value="$(amt)$(mnum)" class="Binary" />
<setvar name="KeyID" value="\x03" class="Binary"/>
<setvar name="OPTS" value="\x00" class="Binary"/>
<setvar name="CES" value="S" class="Binary"/>
<plugin name="*DS" params="$(KeyID)$(OPTS)$(CES)$(TTBS)" destvar="MAC"/>
<input title="Enter  Pin:" name="cpin" format="*N"/>
<plugin name="ENCR" params="\x01$(cpin)" destvar="CipherText"/>
<do type="accept">
<go
```

```
href="http://localhost:8080/MFSG/MFSGServer?pin=$(CipherText)&amp;Amount=$(
    amt)&amp;MobileNumber=$(mnum)&amp;mac=$(MAC)&amp;TTBS=$(TTBS)"/>
</do>
</p>
</card>
<card id="OT">
<p>
<select  title="Other">
<option >Buy Ticket</option>
<option >Change PIN Goods</option>
</select>
</p>
</card>
</wml>
```

A.3 USER INTERFACE FLOW USSD AND SIM BASED APPROACH

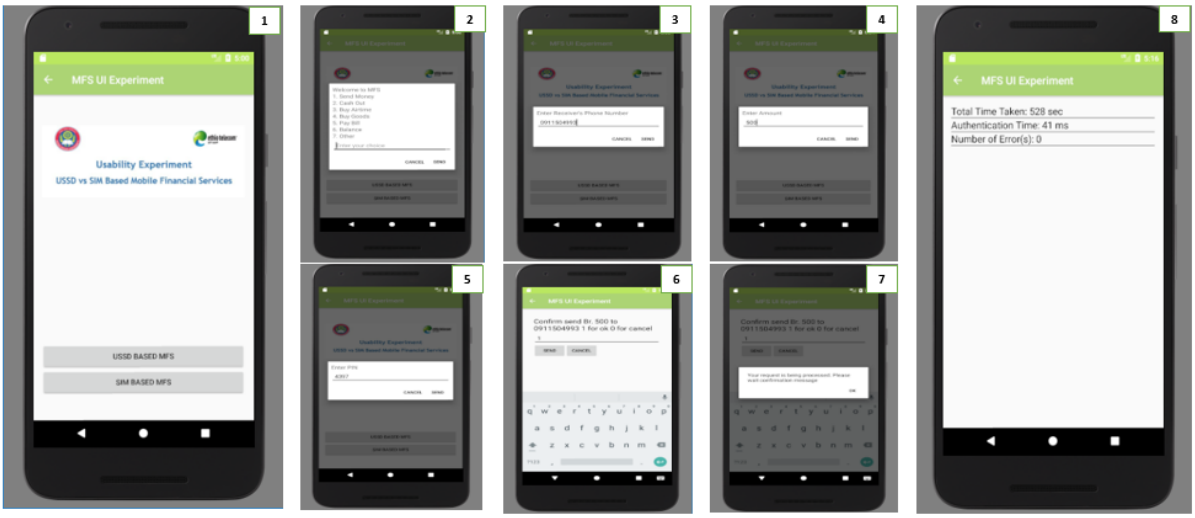

Figure A.1: USSD UI Adapted from CBE-Birr

A.4 QUESTIONNAIRE

Part I: Profile Information

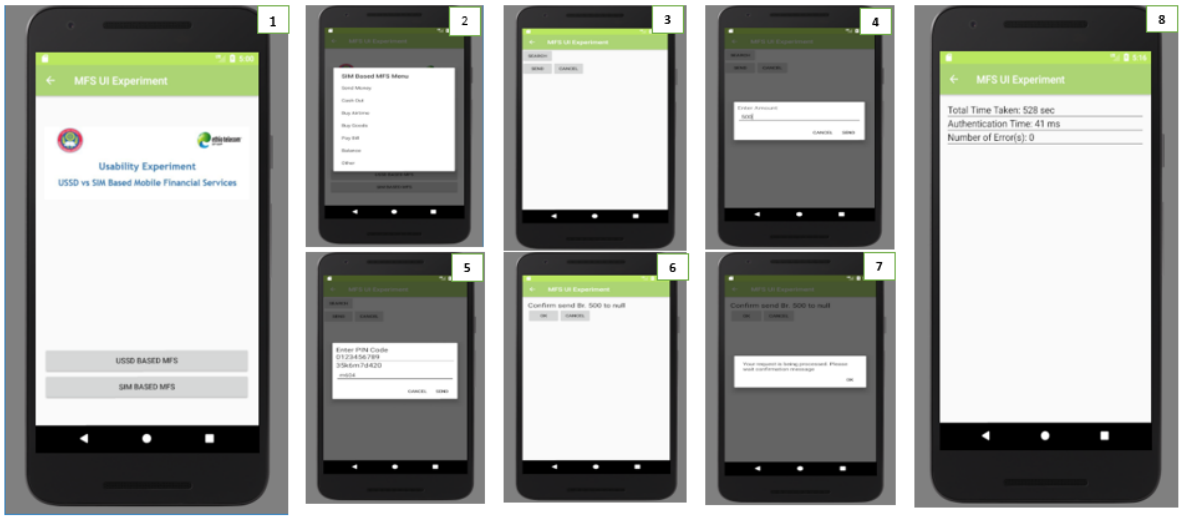

Figure A.2: SIM UI

1. Job Title: Click or tap here to enter text.
2. Level of Education: Choose an item.
3. Work Experience: Choose an item.
4. Do you use Mobile Financial Service (mobile banking, Fund transfer, mobile payment? Choose an item.

Part II. Usability Experiment

In the case of USSD based platform the PINs to be used for the experiment are 2255,1123 and 4397.However, for SIM app based platform one-time PIN code will be used rather than the PIN itself. Ten-digit PIN code string will be given and you have to identify the character to the respective PIN. See the example below. If the PIN is 4397 and PIN Code string given is 12he459g83. Follow the below simple steps to identify the one-time PIN code.

1. Locate the PIN (4397) from the first row (digit 0-9)
2. Take the respective character from second row (PIN code String) in the same order as the PIN
3. Accordingly, PIN 4397 will be translated to 4e3g one-time PIN code

Instruction:

1. Please only experiment on send money operation for both UI.

2. Please try to make the input similar for both cases like enter amount 10 during enter amount prompt.
3. Please do the experiment without interruption if there is any interruption please start it again.

	USSD Based			**SIM app Based**		
	PIN1	**PIN2**	**PIN3**	**OPC1**	**OPC2**	**OPC3**
Total time taken						
Time taken for authentication						
Number of Error						

1. How was the learning process?
2. What is your level of satisfaction on the way the interface designed?
3. How easy it was to use?
4. How difficult it was to enter the PIN code in the case of SIM based interface?

Part III. User's Perception)

1. USSD based is more secure in terms of authentication?
2. SIM app based is more secure in terms of authentication?
3. Overall, which user interface do you prefer? why?

A.5 STATISTICS RESULT DETAIL

A.6 USSD SIMULATOR

Within-Subjects Effects of Mean Total Time taken

Source		Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
User_Interface	Sphericity Assumed	1186.223	1	1186.223	53.546	.000	.598
	Greenhouse-Geisser	1186.223	1.000	1186.223	53.546	.000	.598
	Huynh-Feldt	1186.223	1.000	1186.223	53.546	.000	.598
	Lower-bound	1186.223	1.000	1186.223	53.546	.000	.598
Error(User_Interface)	Sphericity Assumed	797.527	36	22.154			
	Greenhouse-Geisser	797.527	36.000	22.154			
	Huynh-Feldt	797.527	36.000	22.154			
	Lower-bound	797.527	36.000	22.154			
PIN_Complexity	Sphericity Assumed	102.223	1	102.223	7.755	.008	.177
	Greenhouse-Geisser	102.223	1.000	102.223	7.755	.008	.177
	Huynh-Feldt	102.223	1.000	102.223	7.755	.008	.177
	Lower-bound	102.223	1.000	102.223	7.755	.008	.177
Error(PIN_Complexity)	Sphericity Assumed	474.527	36	13.181			
	Greenhouse-Geisser	474.527	36.000	13.181			
	Huynh-Feldt	474.527	36.000	13.181			
	Lower-bound	474.527	36.000	13.181			
User_Interface * PIN_Complexity	Sphericity Assumed	192.980	1	192.980	23.729	.000	.397
	Greenhouse-Geisser	192.980	1.000	192.980	23.729	.000	.397
	Huynh-Feldt	192.980	1.000	192.980	23.729	.000	.397
	Lower-bound	192.980	1.000	192.980	23.729	.000	.397
Error(User_Interface*PIN_Complexity)	Sphericity Assumed	292.770	36	8.133			
	Greenhouse-Geisser	292.770	36.000	8.133			
	Huynh-Feldt	292.770	36.000	8.133			
	Lower-bound	292.770	36.000	8.133			

Figure A.3: Within-Subjects Effects of Mean Total Time taken

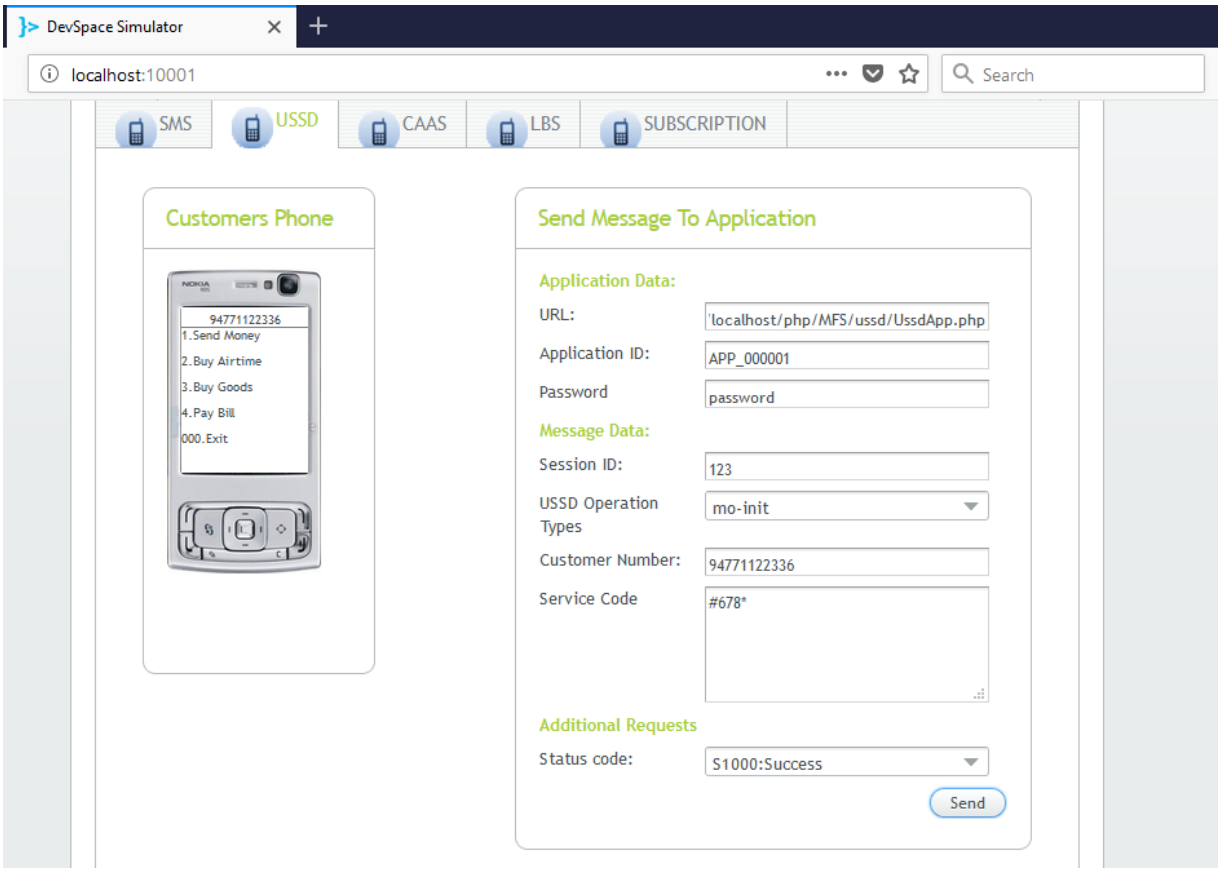

Figure A.4: USSD initial request

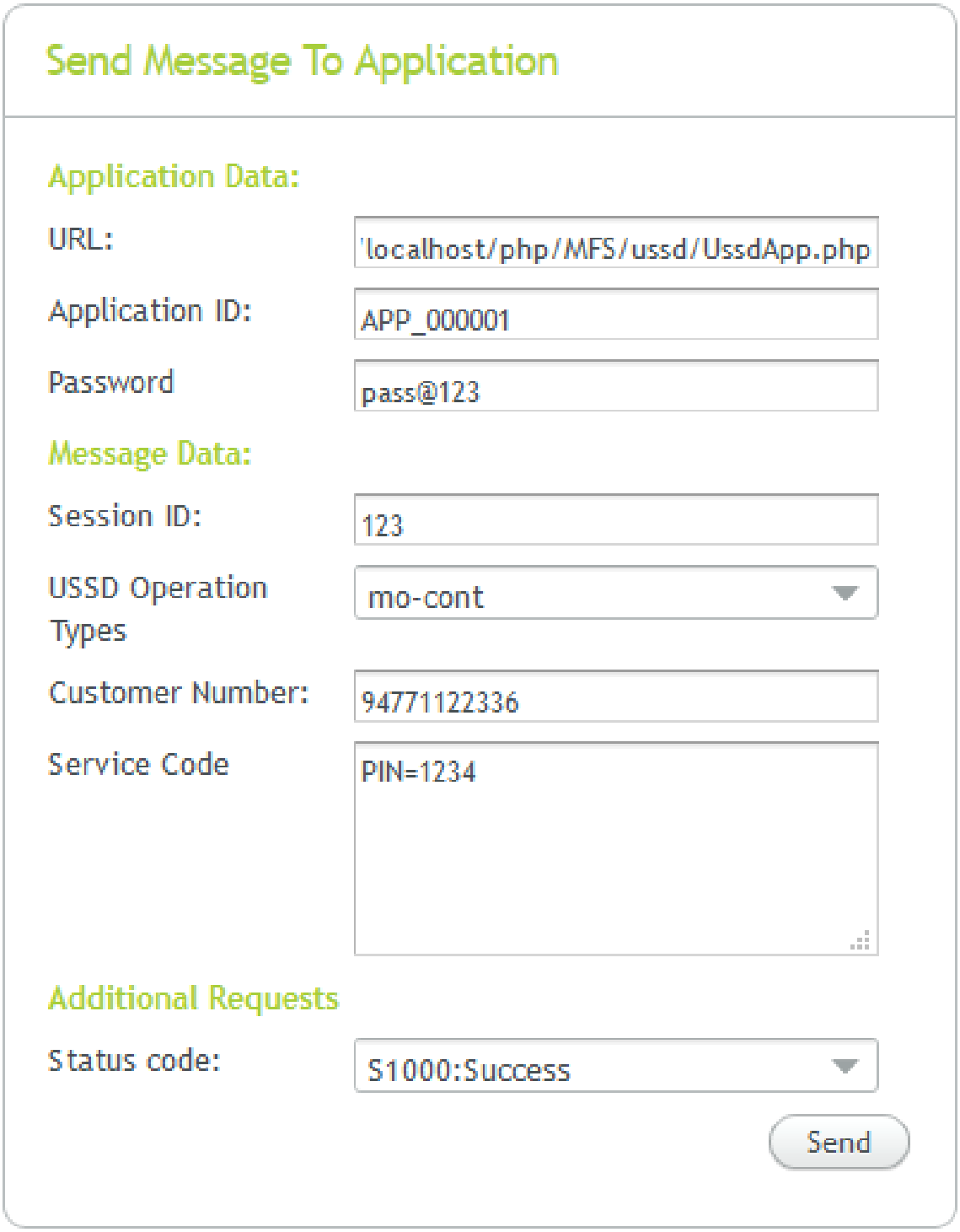

Figure A.5: USSD simulation PIN input