Secure Mobile Payment System Using Symmetric Cryptography in Ethiopia

Saron Hadelo
HiLCoE, Software Engineering Programme, Ethiopia
New Age IT Solution, Addis Ababa, Ethiopia
sarone4@gmail.com

Taye Abdulkadir
HiLCoE, Ethiopia
tabdulkadir@ieee.org

Abstract

Mobile payment allows users to perform payment transactions through their mobile phones. However, security issues are by far the greatest deterring factors that limit the popularity of this payment system. The problem is lack of sufficient security mechanisms with existing mobile payment systems, mainly due to improper protocol design and the deployment of lightweight cryptographic operations which lead to lack of important transaction security properties. The paper uses various research techniques, including questionnaire and interviews to find out the challenges to the adoption of Mobile Payment Systems (MPS) in Ethiopia, and propose solutions to encourage user acceptance of this platform as a convenient alternative payment system. In doing so, we propose a more secured MPS. Mobile phones present an enormous opportunity for use as platforms for a "Payments System". Traditionally in Ethiopia, financial transactions are made using physical cash or cheque. However, from the survey conducted as part of this research, people are willing to use MPS on their phones as far as proper security mechanisms are put in place and the associated risk is reduced. As part of the research, a symmetric cryptography protocol/framework has been developed. To demonstrate the implementation of the MPS with appropriate security features in place, an application prototype has also been developed.

Keywords: Mobile Payment System; Mobile Payment Protocol; Symmetric Cryptography

1. Introduction

According to the World Bank's World Development Indicators, mobile subscription per 100 people in Ethiopia has reached 27 in 2013, and the trend is growing year by year [1]. The widespread reach and expansion of mobile phones is spearheading as the effective media to reap the benefits for transferring money from mobile handsets without visiting a bank.

Mobile payment (also referred to as mobile money, mobile money transfer or mobile wallet) generally refers to payment services operated under financial regulation and performed from or via a mobile device. Also, the mobile payment as an important part of m-commerce is defined as the process of two participants exchanging monetary values employing a mobile device in response for merchandise or services [2]. Mobile Payment is an area which is experiencing rapid developments in the last few years in different countries of the world. The success story of M-Pesa in Kenya is one of the fairy-tale stories. Mobile phones are becoming more and more one's wallets that carry cash to transact at virtually any place.

Mobile Payment System (MPS) is an innovative application on the mobile phone platform that allows a person to initiate a transaction and make a payment using a mobile phone. MPS, as an emerging payment system, allows commercial transactions to be carried out anytime, anywhere and by anyone [3]. In Ethiopia, as elsewhere in Africa, the common payment system used by the majority of the population is cash payment system, where physical cash is used to pay for transactions. However, there are other payment systems such as Card Payment System, Online Payment System, and Mobile

Payment System. But, these payment systems are yet to start and gain acceptance in Ethiopia.

Even if it has the potential of driving an economy towards a cashless society, security issues are one of the major challenges for the new mobile commerce sector. Mobile security is considered to be a major issue for mobile payment that can be faced through sensitive payment. Actually, there are many research papers discussing businesses, markets, payment processing and payment schemes [4], but in fact there are few papers that deal with the construction of wireless payment schemes, involving protocols and security protection solutions [5]. Mobile payment applications face security risks such as insufficient transport-layer protection, poor authorization and authentication, broken cryptography, sensitive information disclosure, etc. [6]. When shopping using a mobile Internet browser, it is required to provide a payment method which is both practical and secure.

The focus of this paper is on Mobile Payment Systems, to look at mobile payment and its security. Applications used for financial transactions need to be more reliable and have end-to-end security. In order to protect mobile applications and data being transferred from these applications, a number of security measures are taken in advance. Cryptography is one of the essential techniques to maintain confidentiality in mobile applications.

This paper presents a secure mobile payment system which is suitable for mobile commerce to transfer payment using symmetric cryptography based on substitution cipher which requires lower computation at all engaging parties (client, merchant, and payment server).

2. Related Work

In today's society, mobile telephony is taking over and has allowed people to do different things from social networking, art, through photography, information retrieval, shopping and carrying out financial tasks as well. Mobile wallets, being one of these favorable features, allow individuals to bank using their mobile phones even in remote villages. Not only are people able to carry out their finance related activities through mobile money transfers, but also the feature has played an important role in helping to develop digital finance and banking as a whole.

Indeed, it has proven to be one of the most effective forms of banking. This is mostly in the developing countries, where there is little or no access to the Internet. Another upside of mobile money transfer is that, in contrast to the formal banking system, this form of banking in general requires little operational knowledge and has less strict rules. For instance, formal banking has "know your customer" rule which does not necessarily apply to mobile money transfer. Little information about a user is required from the subscribers who only agree to the terms of use as per the contract of the subscription.

In Europe, the growth of mobile based money transfers has experienced little or no growth at all [6]. On the other hand in Kenya, Brazil, and India, telecommunication companies and banks have promoted financial aptitude among individuals in the remote areas to reach a wider population. Kenya's Safari-com does this through M-pesa services run by agents who include shopkeepers in towns and entrepreneurs running small businesses countrywide.

In a recent research [8], it was suggested that technological change in the form of less expensive phones and expanded network coverage made mobile money feasible. The most basic technology used for long-distance fund transfer is Short Message Service (SMS). The next technology, which is more user-friendly, is the Unstructured Supplementary Service Data (USSD), which gives some prompts for funds transfer. This technology is still in use by some Mobile Network Operators (MNOs). Another technological channel used for mobile money service is the more sophisticated SIM Toolkit Application (STK), an application encoded in a Subscriber Identity Module (SIM) Card, a portable memory chip used in some mobile phones, which has better network security [9].

Despite all the technological advancement in mobile technology, security is still an important issue with m-payment. For example, near-field communication (NFC) has been identified to have the vulnerability of a man-in-the-middle attack, in which an attacker could intercept exposed information during the communication with the reader, which is usually within 10 cm radius [10]. Basic phones with mobile money capability could be described as GSM (Global System for Mobile) compatible phones with embedded services such as SMS and USSD [10]. There is, however, no end-to-end security for SMS, protection in the GSM or UMTS (Universal Mobile Telecommunications System) network. Furthermore, USSD has no separate security properties; instead it relies on the GSM/UMTS signaling plane security mechanism (just like SMS). It is further argued that the security mechanisms of authentication, message integrity, replay detection and sequence integrity, proof of receipt and proof of execution, message confidentiality and indication of security mechanisms exist. However, it depends on the applications whether these security mechanisms are implemented and whether their cryptographic strength is sufficient [11].

3. The Proposed Solution

3.1 The Proposed Symmetric Encryption

This research uses symmetric cryptography (substitution named *Mesgiti*) to secure mobile payment protocol. Even if there are much more techniques for symmetric encryption, we use a new symmetric encryption technique to make the protocol suitable for the Amharic language.

All forms of cryptanalysis for symmetric encryption try to exploit the fact that traces of structure or pattern in the plaintext may survive encryption and be discernible in the cipher text. In simple substitution ciphers, each plain text character is replaced with fixed cipher text character. But this mechanism is weak from statistical analysis methods whereby considering the rules of the language, the cipher can be broken.

This paper proposes the *Mesgiti* symmetric encryption/decryption algorithm based on substitution mapping. It is a symmetric algorithm, that means the same key is used for encryption and decryption. It is a block encryption algorithm which uses 128 bit key. *Mesgiti* substitution technique is one in which the letters of the plaintext are replaced by other letters or by numbers. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns. Here each alphabet/letter of plain text is replaced by numerical/number value and the number replaced by letter. Thus the cipher text obtained becomes computationally infeasible to break without knowing the key. The algorithm is given in Algorithm 1.

Algorithm 1: *Mesgiti* Substitution Cipher

Notation:

P = Plaintext

C = Ciphertext

K = Key

L = Letter

N = Number

EL = Exact Letter assigned for number, e.g., 1=a, 2=b, 3=c, ...

EN = Exact Number assigned for letter, e.g., a=1, b=2, c=3, ...

FL = First Letter of the alphabet, e.g., a= a is first letter of the English alphabet

FN = First Number, e.g., 1= 1 is first number

FFL = First letter found by calculation

FFN = First number found by calculation

GL = Given letter assigned to the key number, e.g., 2=d

GN = Given number assigned to the key letter, e.g., f=10

NL = The letter which is needed, e.g., find m? answer m=20

NN = The number which is needed, e.g., find 8? answer 8=g

n0 = number of zero

X_K = X of the key, X may be GL, GN, EL, EN, FFL or FFN

X_L = X of the Letter, X may be GL, GN, EL , EN, FFL or FFN

X_N = X of the Number, X may be GL, GN, EL, EN, FFL or FFN

1. Replace letter with number and number with letter
   // Give numerical values for letter L = 0 to infinite, assign number to letter and give alphabetical values for number N='a' to 'z', assign letter to number (English letter) and N='ሀ' to 'ፐ' (Amharic letter)
2. Given EV (exact value) for letters and numbers, given value should be constant
   // Exact number for each letter and vice versa, this given exact value is constant which can be used to make calculation for encryption and deception
3. Represent the value with another value to make it secret, GV (given value) for letters and numbers, given value should not be constant
   // Give number for each letter and vice versa, this given value is secret key which can be used to make calculation for encryption and deception.
4. Find value (FV) of the needed value (NV) for making encryption/decryption
   // Select secret key: kept secret by the two parties to encrypt communications, each party can be confident that it is communicating with the other as long as the decrypted messages are meaningful
   // Encrypt the plaintext
      – For letters: encrypt letter into number
        $FL = (GN_K - EN_K) + 1$
        $NL = (N_{FFL} + EN_L) - 1$
      – For number: encrypt number into letter
        $FN = (GL_K - EL_K) + 1$
        $NN = (L_{FFN} + EL_N) - 1$
   // Decrypt the ciphertext
      – For letter: decrypt letter into number
        $FFL_{FN} = (EN_K - GN_K) + 1$
        $N_{NL} = (NL - FFL) + 1$, to find any number of a given letter except 0
        $N_{NL} = (NL - FFL) + (n0 * n0 + n0)$, used only to find number of 0, use the exact number of '0' to make calculation except 1 and 2, for this number multiply n0 by 0
      – For number: decrypt number into letter
        $FFN_{FL} = (EL_K - GL_K) + 1$
        $L_{NN} = (NN - FFN) + 1$
   // Rule**:**
      – Count forward if you get negative number
        Example: let the key be d=1, a=-2, b=-1, c=0, d=1, ...
      – Back to 'a' after reaching 'z 'or back to 1 after counting 26 (English) and back to 'ሀ' after reaching 'ፐ 'or 1 after counting 34 (Amharic)
        Example: let 1=s, 2=t, ... 8=z, 9=a
      – Use approximate number for number of zero, 0<0.5<1→0_0.5=0 and 0.5_1=1
        Example: Founded 'ሐ' is 41→ ሐ=40=4(0)

3.2 The Proposed Mesgiti Mobile Payment (MP) Protocol

Secure payment systems are critical to the success of mobile commerce. There are four essential security requirements for safe mobile payments, namely, authentication, encryption, integrity and non-repudiation. Encryption is the key security scheme adopted for mobile payment systems, which is used in protocols like SSL (Secure Sockets Layer) which is widely deployed today on the Internet and has helped create a basic level of security sufficient to begin conducting business over the Web.

Mesgiti MP Protocol offers the ability to perform payment transactions on limited computational capability devices (mobile phones). It deploys symmetric key operations and keyed-hash functions to reduce the computation at engaging parties. It also keeps transaction privacy by transferring payment-related information of engaging parties in ciphertext during transactions.

The proposed protocol is composed of three engaging parties: client, merchant, and bank. At the beginning of the protocol, the client and merchant exchange the necessary information to start the

protocol. Then the client requests the bank for authorization to perform the transaction.

The bank checks the validity of the client's account and the amount requested by the client. Meanwhile, the bank sends the confirmation request to the client, then after confirmation, deducts the amount from the client's account and transfers the amount to the merchant's bank. Finally, the bank sends payment notification to client and merchant. The proposed *Mesgiti* Mobile Payment (MP) Protocol is shown in Figure 1.

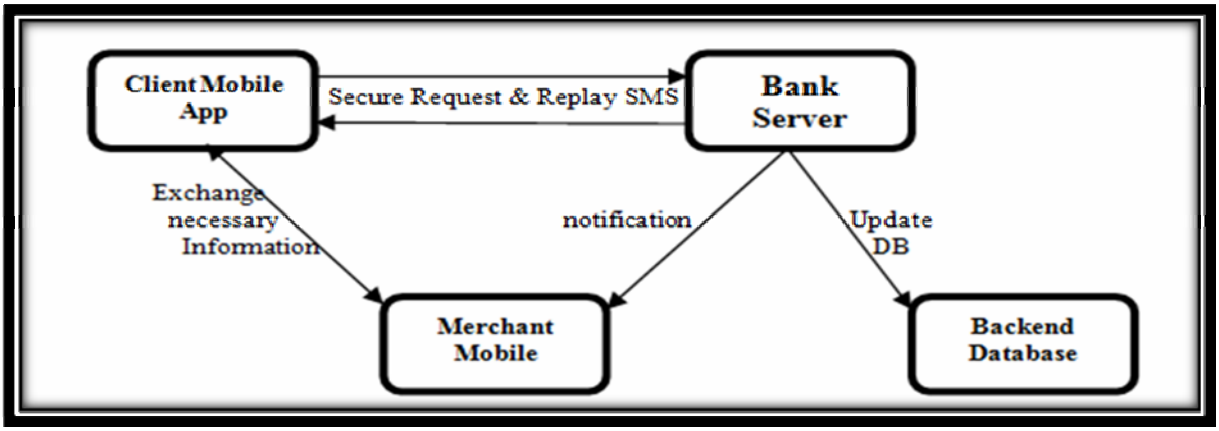

Figure 1: Overview of *Mesgiti* Pay MP Protocol

3.3 MesgitiPay Prototype

MesgitiPay mobile payment app is an easy, fast and secure system that provides the options to charge a customer anywhere and anytime. It provides an easy-to-use user interface as part of the average user's mobile environment, which will be used for collecting user inputs and processing them. The system provides an interface for the user for transaction processing information once the registration information and account creation process with a bank is finalized. The application interface class is responsible for the interaction between the client and banking application. The user interface consists of J2ME GUI components like Forms, Buttons, Canvas, TextBox, TextField, AlertBoxes and Lists. The system provides user freedom such as to cancel a transaction, adding or deleting a service provider (bank) or beneficiary from the "Bill Payment List".

This section summarizes the user interface developed for the prototype application as a demonstration of what users see on the screen of their phones.

The login screen is shown in Figure 2. The prototype is shown in Figure 3 and the main view in the application is shown in Figure 4. The bank keeps track of the client's balance. In addition, clients check their balance in their account. The interface presents two action buttons to check balance and transfer money, which respectively run the balance and transfer money protocols for a single transaction.

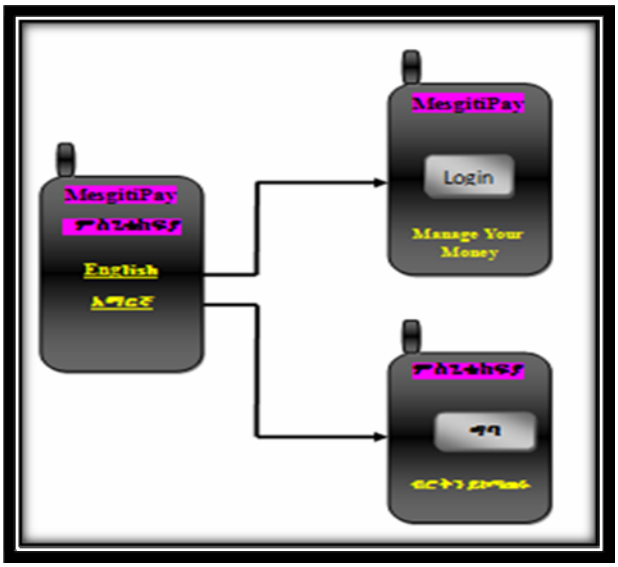

Figure 2: Login view of *MesgitiPay* Prototype

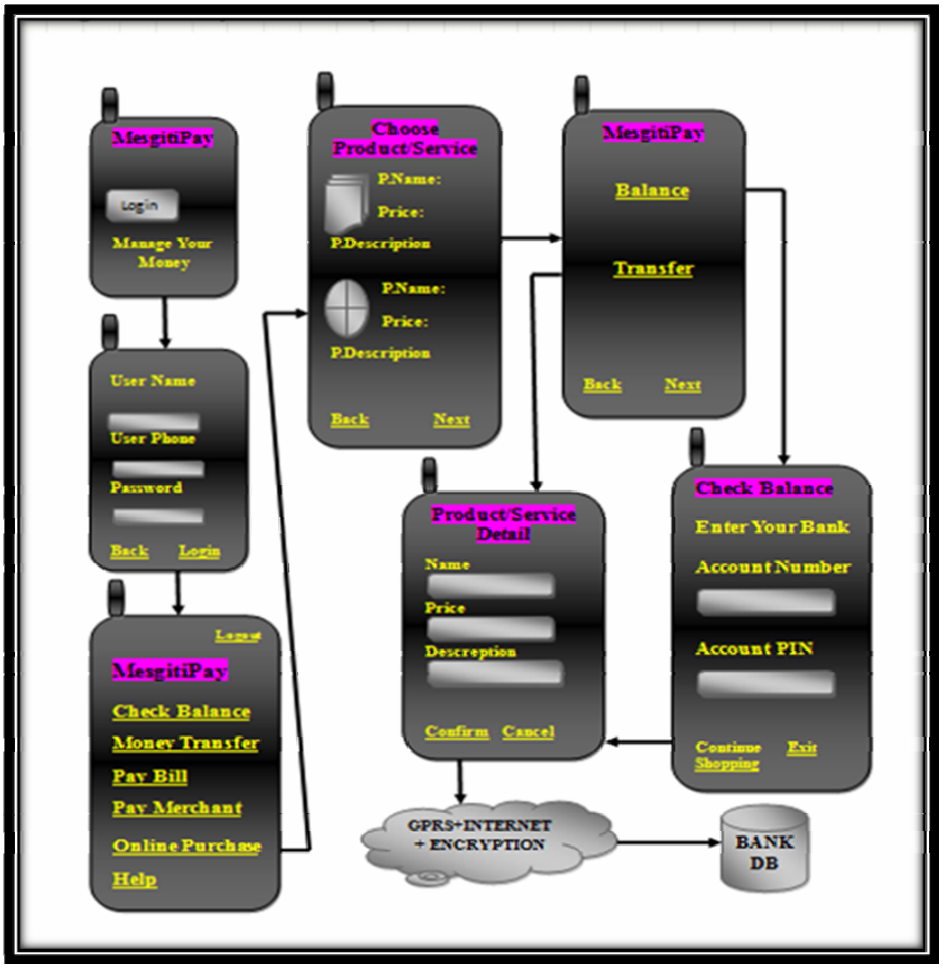

Figure 3: MesgitiPay Prototype

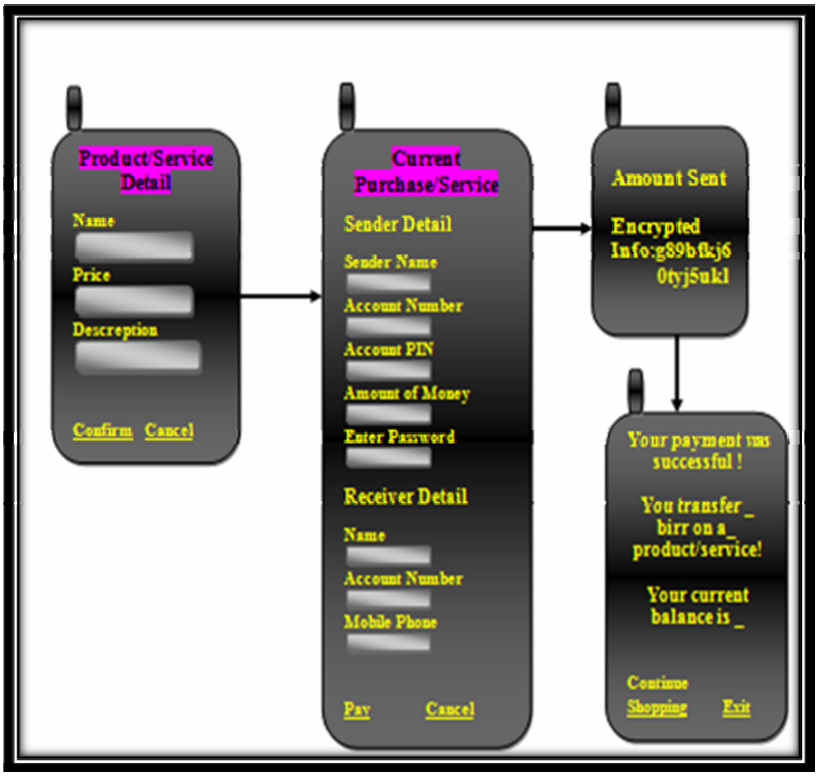

Figure 4: Main view of *MesgitiPay* Prototype

4. Conclusion and Future Work

This paper proposed a practical and secure mobile payment framework for payment transactions - symmetric encryption for a practical and secure mobile payment system which is suitable for Amharic language. We designed secure mobile payment protocols and designed a prototype (*MesgitiPay*). The proposed development of lightweight cryptographic algorithms is guaranteed to be able to increase transaction security and performance while applying them to the proposed mobile payment protocols.

This paper serves as an initial step in addressing the different aspects of MPS in Ethiopia so that this potent mode of transaction becomes common place. The following are future research works:

- Further in-depth studies in security protocols, especially focusing on different Ethiopian languages,
- End to end simulation of MPS through development of high end prototypes,
- Studies on MPS security risks by studying a wide range of the population, and
- Comparison of MPS against other forms of payment by taking a wide range of factors into consideration.

References

[1] Worldbank, http://data.worldbank.org/indicator/IT.CEL.SETS.P2

[2] Nambiar, S. and Liang, L., IEEE IRI, 8-10, 475-480, November 2004.

[3] Deans, P. C., “E-Commerce and M-Commerce Technologies”, IRM Press, 2005.

[4] L. Antovski, and M. Gusev, “M-Payments”, Proceedings of the 25th International Conference on Information Technology Interfaces, 2003.

[5] X. Zheng, and D. Chen, “Study of Mobile Payments System”, Proceedings of the IEEE International Conference on E-Commerce, 2003.

[6] A. K. Jain and D. Shanbhag, “Addressing Security and Privacy Risks in Mobile Applications,” IT Prof., Vol. 14.

[7] The Economist, “Mobile-money services: Let us in” http://www.economist.com/node/21560878, 2012.

[8] World Bank, Information and communications for development 2012: Maximizing Mobile, http://www.worldbank.org/ict/IC4D2012, 2012.

[9] IFC (International Finance Corporation), Mobile Money Study, http://www.ifc.org/ifcext/globalfm.nsf/Content/Mobile+Money+Study+2011, 2011.

[10] Lee, Y. S., Kim, E. and Jung, M. S., “A NFC based Authentication method for defence of the Man in the Middle Attack”, 3rd International Conference on Computer Science and Information Technology (ICCSIT'2013), 2013.

[11] Schwiderski-Grosche, S. and Knospe, H., “Secure M-Commerce”, Information Security Group, Royal Holloway University of London, UK., 2002.