

**Implementing Timestamps with Personal Identification Number (PIN)
Mechanism to Enhance PIN to Provide Non-Repudiation in Mobile
Payment Systems**

Isaac Kega Mwangi

**A thesis submitted in partial fulfillment for the degree of Master of Science in
Software Engineering in the Jomo Kenyatta University of Agriculture and
Technology**

2013

DECLARATION

This thesis is my original work and has not been presented for a degree in any other university.

Signature:  _____

Date: 7/11/2013

Isaac Kega Mwangi


This thesis has been submitted for examination with our approval as the university supervisors

Signature:  _____

Date: 7/11/2013

Dr. Joseph Wafula Muliaro

JKUAT, Kenya

Signature:  _____

Date: 7/11/13

Dr. Stephen Kimani

JKUAT, Kenya

DEDICATION

I would like to dedicate this work to God and my parents Mr. Vincent Mwangi Kega and Mrs. Jemima Wasai Mwangi for their support in ensuring that I complete this degree not only in monetary terms but also in their advice ,emotional support and prayers they showered me with to enable me to complete this course

ACKNOWLEDGEMENTS

I wish to sincerely thank my brother David and sister Alice for their prayers and words of encouragement they gave me during the conducting of this project and all my friends who also encouraged me throughout the whole duration of the project.

I wish to also sincerely thank my supervisor Dr. Joseph Wafula Muliaro for his unwavering support during the planning and execution of the system experiments, his guidance, patience and availability, Dr. Stephen Kimani for his scientific and technical guidance throughout the course of research, data analyses, system design and writing of the thesis.

I would also like to thank the staff of the Institute of Computer Science and Information Technology for their support in setting up presentations that helped me knowing how to conduct the research throughout the whole period and the business fraternity of Thika town where I conducted my research mostly.

TABLE OF CONTENTS

DECLARATION	Error! Bookmark not defined.
DEDICATION	iii
ACKNOWLEDGEMENTS	iv
LIST OF FIGURES	x
LIST OF TABLES	xii
LIST OF APPENDICES	xiii
LIST OF ACRONYMS	xiv
ABSTRACT	xv
CHAPTER ONE	1
INTRODUCTION	1
1.0 Back Ground Information	1
1.1 Problem Statement	3
1.2 Purpose Of The Study/General Objective.....	4
1.3 Specific Objectives.....	4
1.4 Research Questions	5
1.5 Justification	5
1.6 Area Of Study/Scope.....	6
CHAPTER 2	7
LITERATURE REVIEW	7
2.0 Introduction	7
2.1 Technologies For Mobile Payment	7
2.2 Mobile Payment System Types.....	10

2.3 Authorization Mechanisms Employed In Mobile Payment Applications	12
2.4 Pin Algorithms	14
2.4.1 Ibm Pin Algorithms.....	14
2.4.2 Visa Pin Algorithm	18
2.5 Non Repudiation	21
2.5.1 Ways In Which Non-Repudiation Is Employed Currently In Mobile Payment Systems.	21
2.5.2 Categories Of Non-Repudiation:	27
2.5.3 Mechanisms For Providing Non-Repudiation	29
2.6 Development Platforms For M-Payment Application Development.....	31
2.6.1 C # (Sharp).....	31
2.6.2 Java.....	32
2.6.3 C++ Language.....	32
2.7 Existing Mobile Payment Applications	33
2.7.1 Mpesa	33
2.7.2 Paybox.....	35
2.7.3 M-Pay.....	37
2.7.4 Vodafone M-Paybill.....	39
2.8 Conclusion	41
CHAPTER THREE	43
METHODOLOGY.....	43
3.0 Introduction.....	43
3.1. Waterfall Methodology	43
3.1.1 Why Choice In The Waterfall Model.....	47
3.2 Research Design.....	47
3.3 Target Population	47
3.4 Sample Size And Procedures	48

3.5 Data Collection And Data Analysis	48
3.5.1 Data Collection Techniques	49
3.5.2 Data Analysis	50
CHAPTER FOUR.....	52
ANALYSIS AND RESULTS.....	52
4.0 Introduction	52
4.1 Knowing The Percentage Of The Respondents Who Use Mobile Payment In Their Business.	52
4.2 Age Distribution Of The Respondents.....	53
4.3 Education Level Of The Respondents	54
4.4 Respondents Experience In Using Mobile Payment.....	56
4.5 Gender Distribution Of The Respondents.....	57
4.6 Respondents Knowledge Of Authorization And Non-Repudiation Mechanisms	58
4.7 Security Challenges in Mobile Payment.	61
4.8 Measures To Curb The Security Challenges By Mobile Service Providers	62
4.9 Respondent’s Attitude Towards Current Mobile Systems.....	63
4.10 Does Education Level Affect The Use Of Mobile.....	65
4.11 Education Level Affects The Attitude Of	67
4.12 Do the Respondents Favor the Proposed Approach Of Enhancing Pin.....	68
4.13 Respondents thought on the current safety of transactions.....	70
4.14 Respondents Thoughts On Current Non-Repudiation Mechanisms In Mobile Payment Applications	71
4.15 Conclusion	72

CHAPTER FIVE.....	79
SYSTEM DESIGN.....	79
5.0 Introduction.....	79
5.1. How Analysis Informed My Design Criteria And The Algorithm	79
5.2 Mobile Payment Architecture	80
5.2.1 Conceptual Model For The Mobile Payment System	81
5.3 Architecture For The Proposed Mobile Payment System.....	82
5.4 Pin-Timestamp Algorithm	85
5.5 System Design.....	87
5.5.1 Use Case Diagram.....	87
5.5.2 Sequence Diagram	89
5.5.3 Mobile Payment Request State Diagram	92
5.5.4 Mobile Payment Class Diagram.....	94
5.5.5 Mobile Payment Request Activity Diagram	95
CHAPTER SIX	98
EXPERIMENT AND RESULTS.....	98
6.0 Introduction.....	98
6.1 Goal Of Conducting The Experiment	98
6.1.1 Equipment Used In The Experiment.....	98
6.1.2 Setup And Conducting The Experiment	99
6.2 Experimentation Of The Proposed Application.....	101
6.2.1 Functionality Test	103
6.3 Security Test.....	106
6.4 Screen Shots Of Some System Runs.....	108
6.4.1 Database Screenshot Of The Out-Message Table.....	108
6.4.2 Database Screenshots Of The User Accounts	109

6.4.3 System Interface Screen Shots	110
6.4.4 Screen Shot Of Mobile Payment Process.....	111
6.5 Results Of The Experiment.....	113
CHAPTER SEVEN.....	117
EVALUATION, CONCLUSION AND RECOMMENDATIONS.....	117
7.0 Introduction.....	117
7.1 General Discussion.....	117
7.2 Evaluation	119
7.3 The Enhanced Parts Of The Algorithm.....	122
7.4 Compared To Existing Approaches	123
7.5 Conclusion	125
7.6 Recommendation.....	125
REFERENCES.....	127
APPENDIX	135

LIST OF FIGURES

Figure 2.2.1: Remote M-payment system.....	10
Figure 2.2.2: Proximity m-payment system.....	12
Figure 2.4.1.1: IBM PIN generation algorithm.....	15
Figure 2.4.1.2: IBM PIN verification (Offset) algorithm	17
Figure 2.4.2: Visa PIN algorithm diagram.....	20
Figure 2.7.2: Pay box mobile transaction model	37
Figure 2.7.3: M-pay transaction model.....	38
Figure 2.7.4: Vodafone m-PayBill transaction model	40
Figure 3.1: Waterfall model	43
Figure 4.1: Pie chart for use of mobile payment applications in businesses.....	52
Figure 4.2: pie chart for age of the respondents.....	54
Figure 4.3: Chart for education level of the respondents	55
Figure 4.4: Pie chart for experience in using mobile payment applications	56
Figure 4.5: Pie chart depicting the percentages of the respondents involved in the	57
Figure 4.6: awareness to authorization mechanisms in use	58
Figure 4.6.1: Awareness on non-repudiation mechanisms	60
Figure 4.7: Mobile payment challenges facing users.....	62
Figure 4.9: Respondents response on whether current m-pay systems are safe	64
Figure 4.10: Education level against mobile payment use.....	66
Figure 4.11: Education level against perception of mobile payment.....	67
Figure 4.12: Response of those in favor of enhancing PIN	69

Figure 4.13: Response on safety of mobile payment applications.....	71
Figure 4.14: Response concerning non-repudiation mechanisms.....	72
Figure 5.2.1: Mobile payment Conceptual model.....	81
Figure 5.3.: mobile payment architecture	83
Figure 5.5.1: Mobile payment use case diagram.....	88
Figure 5.5.2: Mobile payment Sequence diagram	89
Figure 5.5.3: Mobile payment request State diagram	93
Figure 5.5.4: Mobile payment Class diagram	94
Figure 5.5.5: Mobile payment request Activity Diagram	97
Figure 6.4.1: Out message table.....	108
Figure 6.4.2: subscribed users account	109
Figure 6.4.3: System interface screen shot.....	110
Figure 6.4.4.1: Screenshot for deposing money.....	111
Figure 6.4.4.2: Screenshot for withdrawal	112
Figure 6.4.4.3: Screenshot for transferring money	112
Figure 6.4.4.4: Successful request Confirmation message	113

LIST OF TABLES

Table 4.1: Frequency distribution of the respondents who use mobile payment.....	52
Table 4.2: frequency distribution for age.....	53
Table 4.3: Education level of the respondents	54
Table 4.4: frequency distribution of the experience level of the respondents	56
Table 4.5: Gender of the respondents	57
Table 4.6: user’s response on their knowledge of authorization mechanisms.....	58
Table 4.6.1: Users response on their knowledge of non-repudiation mechanisms.....	59
Table 4.7: Challenges facing mobile payment users.....	61
Table 4.9: Respondent’s attitude response.....	64
Table 4.10: Crosstab of education level against mobile payment use	65
Table 4.11: Education level and perception of mobile payment use	67
Table 4.12: Those who favor for enhancement of PIN.....	68
Table 4.13: Response on safety of mobile payment application.....	70
Table 4.14: Response concerning non-repudiation mechanisms	71
Table 6.2.1.1: Results for the payment request functionality	104
Table 6.2.1.2: Results for authorization of the request	105
Table 6.2.1.3: Results for committing the payment request	106

LIST OF APPENDICES

Appendix 1: Questionnaire for business owners.....135

Appendix 2: Questionnaire for Mobile Service Providers.....141

LIST OF ACRONYMS

PIN.....	Personal Identification Number
MNO.....	Mobile Network Operator
GSM.....	Global System for Mobile Communications
USSD.....	Unstructured Supplementary Service Data
NRR.....	Non-Repudiation of Receive
NRO.....	Non-Repudiation of Origin
NRT.....	Non-Repudiation of Transit
NRS.....	Non-Repudiation of Submission
MSISDN.....	Mobile Station Integrated Service Data Network
J2ME.....	Java Two Micro-Editions
PC.....	Personal Computer
WAP.....	Wireless Application Protocol

ABSTRACT

There are many mechanisms that can be used to authenticate and authorize transactions in mobile payment applications, but the most common one is the Personal Identification Number mechanism (PIN). PIN is widely used because it is easy to implement, also it is easy for the users to remember a 4 digit number that remembering a password. For these and other more reasons PIN is the mostly used mechanism to authorize transactions in a payment application, but PIN has never been able to provide non-repudiation. Non-repudiation is defined as the act of ensuring that parties that are involved in a transaction do not fault on that transaction. It acts as evidence that indeed a said transaction took place between a set of parties and either of those parties cannot fault on that transaction while authorization is defined as the act of ensuring that only authenticated and authorized persons are able to effect a transaction in an application. Hence the main goal or objective of this project was to enhance PIN to provide non-repudiation through the use of timestamps. Timestamps are one of the mechanisms that can be used to provide non-repudiation in applications. The choice for timestamps was that for each transaction there has to be time split between them, hence to ensure non-repudiation, the issue of time is of great importance not only to the people involved in the transactions but also to the authorities that are called upon incase a fraud case crops up.

CHAPTER ONE

INTRODUCTION

1.0 Back Ground Information

The rapid growth of mobile telephony has fueled the expansion of the mobile commerce (M-commerce). M-commerce refers to e-commerce activities via mobile devices, such as phones or Personal Digital Assistants (PDA's) (Gritzalis et al. 1999). The software development process consists of a systematic series of tasks to create a software system: requirements capture, analysis, design, coding, and testing. In the context of any application it is important to ensure that the personal data are kept secure and available to the entities that are authorized to access it (Gritzalis et al. 1999).

Mobile payment (M-payment) systems are everywhere and they have a large impact on the everyday life of businesses and individuals. This is why according to the Communication Commission of Kenya (CCK) the number of registered mobile payment users is much higher (CCK Q3 2012.). This is due to the fact that nearly three quarter of the Kenyan population own mobile phones and out of this three quarter half of them are registered mobile payment users, which is a very big number. The fact is that is attributed to this high number of people participate in mobile payment is that it is relatively cheap convenient and is accessible all the time even at the comfort of your own home. In the light of ambient, pervasive and ubiquitous computing, this impact is increasing significantly. At the heart of these mobile payment applications, security aspects play a vital role and are thus becoming a central issue in M-payments effective

usage. M-payment applications are required to be secure in order to resist the potential large number of attacks on them. The importance of security in these mobile payment applications is the paramount interest of developers around. With a secure application, the returns from the transactions that shall be shared between the mobile operators, content developer and the business shall be high, and also the trust issues that were witnessed beforehand between people and the businesses shall be a thing of the past.

There are various mechanisms that are used to ensure that any application that deals with money or financial issues is secure. The mechanisms are divided into authentication, authorization and non-repudiation mechanisms for these applications. Authentication refers to the act of ensuring that the right person has access to the application while authorization refers to the act of ensuring that the right person initiates a transaction. Non-repudiation refers to the act of ensuring that parties involved in a transaction or any party that sends a message cannot deny of doing that action. (Coffey, T., & Saidha, P. (1996)).

There are various mechanisms for ensuring authorization and non-repudiation of transactions in mobile payment applications. These mechanisms are like the use of biometrics, PIN's, digital signatures for authorizing transactions while for non-repudiation there is the use of timestamps, digital signatures, public key infrastructures, digital signatures etc. (D. Kugler (2003)). These mechanisms have helped a lot in ensuring that transactions done are safe and secure, in light of this it was possible also to look at the flaws of some of these mechanisms and try and enhance them to provide better security mechanism for these services. The flaw that this project work is based on

is to try and enhance the PIN mechanism to provide non-repudiation services in applications. The application in this light that was chosen to test this phenomena were mobile payment applications because these are the current application that are in use by many financial institutions in the country and is widely used by many people. The main objective of the project was to enhance PIN to provide non-repudiation services in mobile payment applications through use of timestamps from the point the request was authorized rather from the point the transaction is being effected by the application.

Thus the project sought to develop a mobile payment application that has an authorization constraint/mechanism on the application. The authorization mechanism will only allow for a transaction to be processed if it meets the constraints criteria, if not it is discarded. It should also cater for non- repudiation (acts as evidence that a transaction was initiated and either party can't falter on it because if they do legal action shall be taken against them.).

1.1 Problem Statement

Most mobile payment applications use the Personal Identification Number (PIN) as their authorization mechanism. It is widely used because it is cost efficient and easy to use unlike the biometric authorization mechanism. Although it is widely used, there is one aspect of PIN that not been considered apart from authorizing transactions and providing cryptographic capabilities and that is it being able to provide non-repudiation. Non-repudiation services like digital signatures, audit logs, and timestamps ensure that of the two parties involved in the transaction cannot falter on the transaction nor refuse to honor the transaction (Coffey, T., & Saidha, P. (1996)). There is need to ensure that

people who use these applications feel that their transactions are safe and secure. For business people it is highly essential to ensure that non-repudiation is achieved because most of them deal with clients whom they are not conversant with about their paying behaviors thus the need to enhance our applications non-repudiation capabilities. Currently most mobile payment applications provide non-repudiation from the transaction level and not from the authorization level and thus to increase the confidence of the users in these mobile payment applications, it is important to ensure that non-repudiation is provided in the application from the point of authorizing the transaction through to the final stage which is committing the payment.

The purpose of this project was to explore how time stamps could be implemented together with the PIN authorization mechanisms in mobile payment applications to enable PIN to provide non-repudiation.

1.2 Purpose Of The Study/General Objective

The purpose of this project was to explore how timestamps could be used with the PIN authorization mechanisms in mobile payment applications to ensure non-repudiation. Ultimate goal was to develop a prototype that has timestamps as a non-repudiation service integrated into the PIN authorization mechanism of the application

1.3 Specific Objectives

- To investigate on how authorization mechanisms and non-repudiation are being currently implemented together in mobile payment applications
- To develop and test a mobile payment application that has implemented timestamps as a non-repudiation service with the PIN authorization mechanism.

- To formulate an algorithm to implement timestamps together with PIN mechanism (that is the secure time stamps model based on mobile payments).

1.4 Research Questions

- What are the authorization and non-repudiation mechanisms that are employed in mobile payment applications?
- What are the non-repudiation mechanisms that can be used to ensure non-repudiation of transactions done through mobile payment applications or any application?
- How shall timestamps be implemented with PIN to enhance it to provide non-repudiation capabilities?

1.5 Justification

Through this project, a way by which non-repudiation services like timestamps to be implemented with the PIN authorization mechanism will be achieved, it will be easier to develop a mobile payment application that employs use of one mechanism for both authorization and ensuring non-repudiation of its transactions right from the point of authorization up to transaction initiation. This will ensure the robustness of this authorization and security mechanism in the application and thus increase the confidence level of users in the use of the application. Since the use of digital signatures are not fully legislated in most countries nor standardized in countries, most of the mobile payment applications use PIN, thus the need to improve on it to provide non-repudiation.

Thus there is need to ensure that authorization mechanisms also provide non-repudiation services because it will be much easier, cheap and effective to implement both authorization and non-repudiation mechanism together right from the authorization

point through to the transaction commit point. Lastly, non-repudiation evidence generated will be hard to deny if a person defaults because each user has a unique PIN that differentiates them.

1.6 Area Of Study/Scope

The area of study of the project was under security, whereby under security, the project explored means of making the PIN mechanism not only be able to provide authorization capabilities but also provide non-repudiation services as well. This made the mechanism to be more robust in securing transactions done.

The scope of the research was based on the mobile context because that is the new medium for money transactions and it is where the PIN authorization mechanism has not yet been made to provide non-repudiation services

CHAPTER 2

LITERATURE REVIEW

2.0 Introduction

This chapter will review existing literature dealing with technologies used in mobile payment systems, mechanisms for providing authorization and non-repudiation, PIN algorithms as well as tools that can be used in development of mobile payment applications.

2.1 Technologies For Mobile Payment

Mobile payment is a new and rapidly adopting alternative payment method – especially in Asia, Africa and Europe (Funk, J. L. (2005)). Instead of paying with cash, cheque or credit cards, a consumer can use a mobile phone to pay for a wide range of services and digital or hard goods such as:

- Music, videos, ringtones, online game subscription or items, wallpapers and other digital goods.
- Transportation fare (bus, subway or train), parking meters and other services
- Books, magazines, tickets and other hard goods.

The two most widely used standards for m-payment applications are Global System for Mobile communications (GSM) and Code Division Multiple Access (CDMA). GSM based phones use a SIM (Subscriber Identification Module) card which is a detachable smart card containing the user's subscription key used to identify a user. In CDMA based phones, the phone itself stores the subscription key

In Kenya this is mostly found in Mpesa and Zap (now Airtel Money) which enable to send and receive money on their mobile phones, buy goods, pay their electrical bills or water bills and also nowadays include even ATM withdrawals from their respective banks (Mas, I., & Morawczynski, O. (2009).

Technologies for mobile payments:

- Premium SMS based transactional payments
- Mobile web payments (WAP)
- Contactless NFC (Near Field Communication)

Premium SMS/USSD based transactional payments

The consumer sends a payment request via an SMS text message or an USSD to a short code and a premium charge is applied to their phone bill or their mobile wallet. The merchant involved is informed of the payment success and can then release the paid for goods.

Since a trusted delivery address has typically not been given these goods are most frequently digital with the merchant replying using a Multimedia Messaging Service to deliver the purchased music, ringtones, wallpapers etc.

A Multimedia Messaging Service can also deliver barcodes which can then be scanned for confirmation of payment by a merchant. This is used as an electronic ticket for access to cinemas and events or to collect hard goods (Cattan, A, and Tomer B. (2005)).

- **Mobile web payments**

The consumer uses web pages displayed or additional applications downloaded and installed on the mobile phone to make a payment. It uses WAP (Wireless Application Protocol) as underlying technology and thus inherits all the advantages and disadvantages of WAP. However, using a familiar web payment model gives a number of proven benefits (*The real digital divide*, The Economist Mar 10, 2005):

1. Follow-on sales where the mobile web payment can lead back to a store or to other goods the consumer may like. These pages have a URL and can be bookmarked making it easy to re-visit or share with friends.
2. High customer satisfaction from quick and predictable payments
3. Ease of use from a familiar set of online payment pages

- **Contact less Near Field Communication**

Near Field Communication (NFC) is used mostly in paying for purchases made in physical stores or transportation services. A consumer using a special mobile phone equipped with a smartcard waves his/her phone near a reader module. Most transactions do not require authentication, but some require authentication using PIN, before transaction is completed. The payment could be deducted from pre-paid account or charged to mobile or bank account directly (Funk, J. L. (2005)).

2.2 Mobile Payment System Types

M-payment systems are of two types - Remote Payments Systems and Proximity payment Systems. In the former, the payer and the payee are at remote locations, e.g. a customer places an order from his home to a retail store without having to be physically present at the retail store. In the latter, payer and payee are in the same vicinity, e.g. a customer (payer) buys a cup of coffee from a vending machine (payee). As shown in Figure 2.2.1 below, the following steps are typically involved in carrying out a transaction using a Remote m-payment system (S. Fong and E. Lai, 2005):

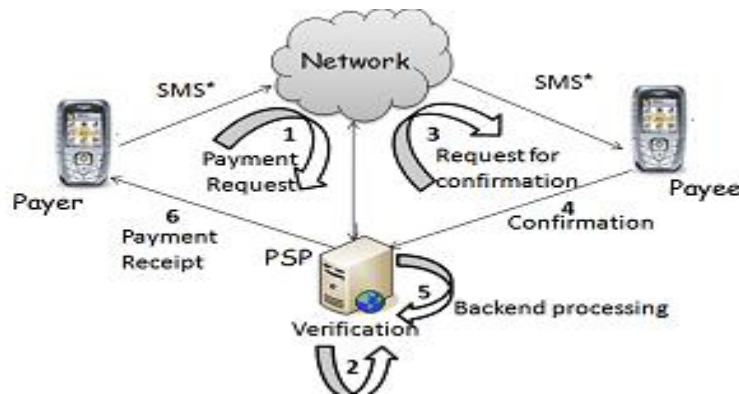


Figure 2.2.1: Remote M-payment system

- The customer uses his mobile device to send a payment request to a PSP (payment service provider) over a wireless network. This request includes the details of the payee and amount to be paid.
- A PSP (payment service provider) verifies the credentials of the customer and the payee (basically it checks whether the customer and payee have registered for such

an m-payment service). Optionally, the PSP might ask the customer for some more details (like a password) for authentication.

- Once the credentials of the customer have been established, the PSP requests the payee for confirmation by forwarding the payment details.
- The payee then sends a confirmation message to the PSP.
- After successful confirmation, the PSP performs backend processing to update the accounts of the payer and the payee.
- It sends a payment receipt to the payer. It might also optionally send a “Transaction completed” message to the payee.

The transaction processing in proximity m-payment systems is similar to the process followed in remote m-payment systems. The main difference lies in steps 1 and step 3. In remote m-payments, the customer first sends the payment request to the PSP over a wireless network by using a remote wireless technology. The PSP then forwards this request to the payee. However, in proximity m-payments, the customer directly sends the payment request to the payee typically using a short-range wireless technology. The payee then forwards this payment request to the PSP over a wireless network. Apart from this classification m- payments can also be categorized based on the payment value involved (Micro, and Macro payments) and the charging method used (Post-paid, Pre-paid, and Pay-now). This is depicted in figure 2.2.2 on the next page. (S. Fong and E. Lai, 2005)

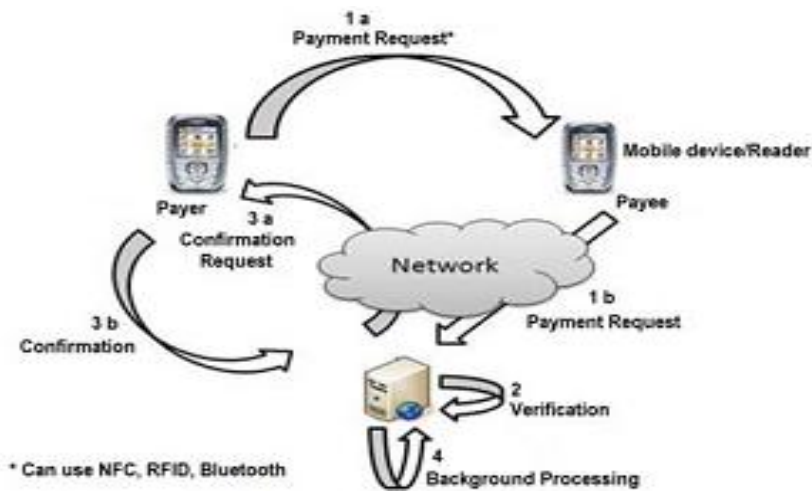


Figure 2.2.2: Proximity m-payment system

2.3 Authorization Mechanisms Employed In Mobile Payment Applications

The following are some of the mechanisms that can be employed in payment authorization:

1. **Digital signatures:** Digital signatures can ensure the authenticity of transaction parties, integrity, and non-repudiation of transmissions. A digital signature is created when the document to be transmitted is enciphered using a private key. The process of enciphering the document using the private key authenticates the document, since the document could only have been enciphered using the private key of the owner. A digitally signed document or message is unalterable after the signature. The recipients can verify the signature by deciphering using the public key. In real world, documents are not completely encrypted to save time. In such cases one-way hash functions are used.
2. **Personal Identification Number (PIN) authorization:** PIN is entered by the user to authorize any operation that needs authorization from either party. The GSM (Global System for Mobile Communications) Subscriber Identity Module

(SIM), which stores personal subscriber data, can be implemented in the form of a special purpose card called SIM card. SIM toolkit is a specification of SIM and terminal functionalities that allow the SIM to take control of the mobile terminal for certain functions. SIM application toolkit (SAT) is used to create Short Message Service (SMS) based mobile payment applications. In SIM Application toolkit based systems, the communication between the mobile client and the payment server occurs using SMS. The SMS is used to initiate and authorize payments.

- 3. Biometric authorization:** This is where for an authorization to be allowed, a person usually can use either one of his/her body parts usually the eyes or fingers to authorize the transaction. The biometric signature of the person is stored in a database usually at the mobile operators servers from where if they want to transact they just put the part needed and the transaction is completed.

(N. J. Park, Y. J. Song. 2001)

2.4 Pin Algorithms

2.4.1 Ibm Pin Algorithms

2.4.1.1: PIN GENERATION ALGORITHM

This algorithm generates an n-digit PIN based on account-related data or person-related data, namely the validation data. The assigned PIN length parameter specifies the length of the generated PIN.

The algorithm requires the following input parameters:

- A 64-bit validation data
- A 64-bit decimalization table
- A 4-bit assigned PIN length
- A 128-bit PIN-generation key

The service uses the PIN generation key to encipher the validation data. Each digit of the enciphered validation data is replaced by the digit in the decimalization table whose displacement from the leftmost digit of the table is the same as the value of the digit of the enciphered validation data. The result is an intermediate PIN. The leftmost n digits of the intermediate PIN are the generated PIN, where n is specified by the assigned PIN length. (IBM PIN). Figure 2.4.1.1 on the next page depicts the steps of the algorithm for IBM PIN generation.

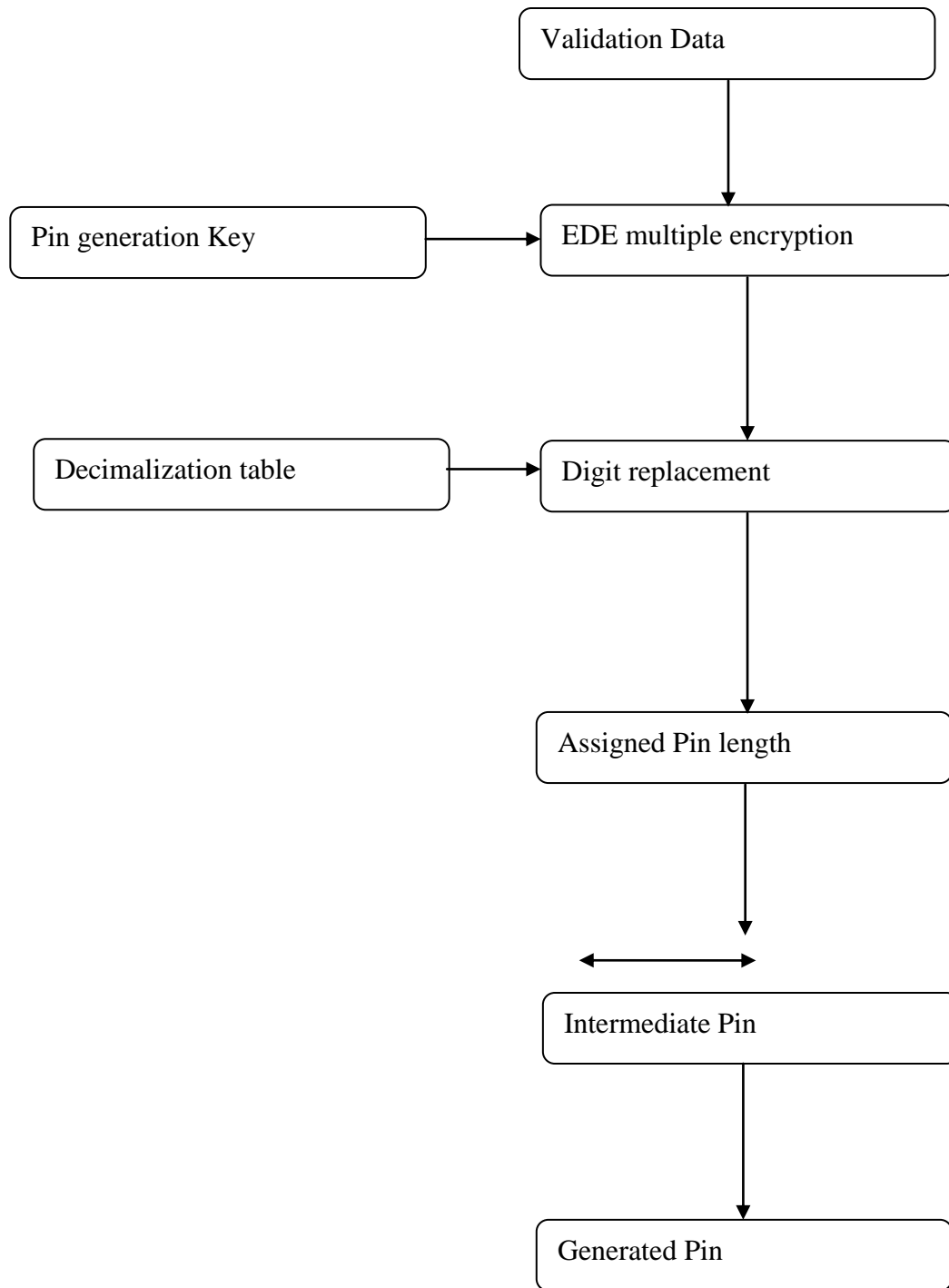


Figure 2.4.1.1: IBM PIN generation algorithm

2.4.1.2: PIN VERIFICATION ALGORITHM

This algorithm generates an intermediate PIN based on the specified validation data. A part of the intermediate PIN is adjusted by adding an offset data. A part of the result is compared with the corresponding part of the customer-entered PIN. The algorithm requires the following input parameters:

- A 64-bit validation data
- A 64-bit decimalization table
- A 128-bit PIN-verification key
- A 4-bit PIN check length
- An offset data
- A customer-entered PIN

The rightmost m digits of the offset data forms the PIN offset, where m is the PIN check length.

1. The validation data is enciphered using the PIN verification key. Each digit of the enciphered validation data is replaced by the digit in the decimalization table whose displacement from the leftmost digit of the table is the same as the value of the digit of enciphered validation data.
2. The leftmost n digits of the result is added to the offset data value, where n is the length of the customer-entered PIN. The addition ignores carries.

3. The rightmost m digits of the result of the addition operation form the PIN check number. The PIN check number is compared with the rightmost m digits of the customer-entered PIN. If they match, PIN verification is successful; otherwise, verification is unsuccessful.

When a nonzero PIN offset is used, the length of the customer-entered PIN is equal to the assigned PIN length. (IBM pin generation algorithm). The algorithm is as shown in the figure 2.4.1.3 below.

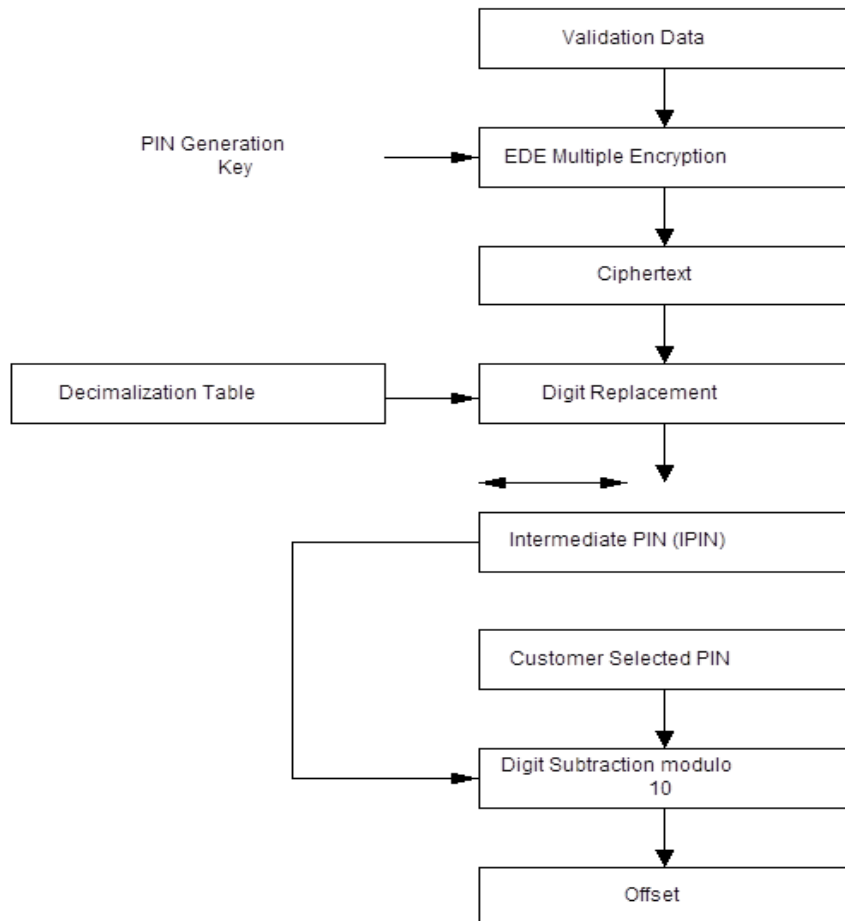


Figure 2.4.1.2: IBM PIN verification (Offset) algorithm

2.4.1.3: PIN OFFSET GENERATION ALGORITHM

To allow the customer to select his own PIN, a PIN offset is used by the IBM® 3624 and GBP PIN generation algorithms to relate the customer-selected PIN to the generated PIN.

The PIN offset generation algorithm requires two parameters in addition to those used in the 3624 PIN generation algorithm. They are a customer-selected PIN and a 4-bit PIN check length. The length of the customer-selected PIN is equal to the assigned-PIN length, n .

The 3624 PIN generation algorithm described above in 2.4.1.1 is performed. The offset data value is the result of subtracting the leftmost n digits of the intermediate PIN from the customer-selected PIN. The subtraction ignores borrows. The rightmost m digits of the offset data forms the PIN offset, where m is specified by the PIN check length. Note that n cannot be less than m . To generate a PIN offset for a GBP PIN, m is set to 4 and n is set to 6. (IBM pin offset algorithm). The above figure 2.4.1.2 of the IBM verification (Offset) algorithm best depicts this algorithm.

2.4.2 Visa Pin Algorithm

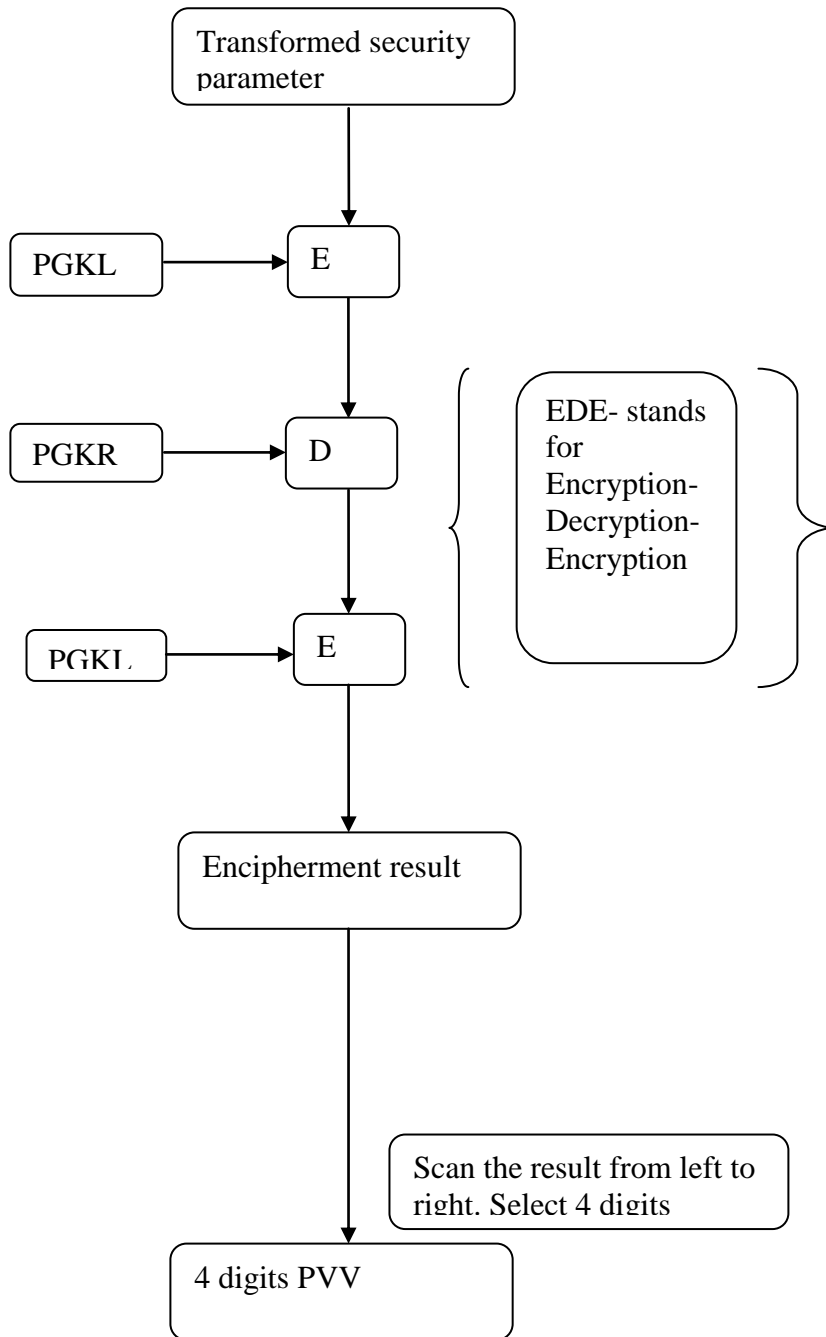
The VISA PIN verification algorithm performs a multiple encipherment of a value, called the Transformed Security Parameter (TSP), and an extraction of a 4-digit PIN Verification Value (PVV) from the ciphertext. (Clulow, J. S. (2003))

The calculated PVV is compared with the referenced PVV and stored on the plastic card or data base. If they match, verification is successful.

The algorithm generates a 4-digit PIN verification value (PVV) based on the transformed security parameter (TSP).

The algorithm requires the following input parameters:

- A 64-bit TSP
 - A 128-bit PVV generation key
1. A multiple encipherment of the TSP using the double-length PVV generation key is performed.
 2. The cipher text is scanned from left to right. Decimal digits are selected during the scan until four decimal digits are found. Each selected digit is placed from left to right according to the order of selection. If four decimal digits are found, those digits are the PVV.
 3. If, at the end of the first scan, less than four decimal digits have been selected, a second scan is performed from left to right. During the second scan, all decimal digits are skipped and only non-decimal digits can be processed. Non-decimal digits are converted to decimal digits by subtracting 10. The process proceeds until four digits of PVV are found. This can be depicted in the figure shown on the next page, that is figure 2.4.2 (Clulow, J. S. (2003))



PGKL: Pin Generation Key Left

PGKR: Pin Generation Key Right

Figure 2.4.2: Visa PIN algorithm diagram

2.5 Non Repudiation

Non-repudiation services establish evidence that establishes accountability regarding a particular event or action. The entity responsible for the action or associated with the event, regarding the evidence generated is known as the evidence subject. Mechanisms for non-repudiation include the following:

1. Timestamps
2. Trusted Third Parties
3. Digital signature
4. Secure audit log

2.5.1 Ways In Which Non-Repudiation Is Employed Currently In Mobile Payment Systems.

2.5.1.1. TIME STAMPS

Time stamps are found in many electronic transactions to indicate the time that a particular event or action took place, e.g. the time that a message was sent or received, the time that a digital signature was generated, or the time that a signature key was revoked. These time stamps may be used to convince other parties involved in a transaction of the validity of an event or action, or used to prove to a third party the truth of an event or action. Users should take care to identify precisely the role of time stamps in a given application. Time stamping is actually thought of as a trusted third party mechanism when it comes to evidence generation. We can time-stamp evidence by

sending it to the time-stamping authority, which appends a time value to the evidence and then digitally signs the result. It is regarded as the legal time of evidence generation and the time at which the time-stamp was applied. (Haber and Stornetta (1997))

In any case, the basic steps implemented by time-stamping services are:

1. The entity sends a digest (hash) of the message to the time-stamp authority. Since the hash does not allow the time-stamp authority to retrieve the original message, the privacy of this message is guaranteed.
2. The time-stamp authority appends (e.g., concatenates) the current time to the received digest and digitally signs this association.
3. The time-stamp authority returns the association and its digital signature. By operating in this way, the user can prove that the message existed at the time specified in the time-stamp by verifying the digital signature of this time-stamp.

This data is usually presented in a consistent format, allowing for easy comparison of two different records and tracking progress over time; the practice of recording timestamps in a consistent manner along with the actual data is called time-stamping.

Timestamps are typically used for logging events or in a sequence of events (SOE), in which case each event in the log or SOE is marked with a timestamp. In file systems, timestamp may mean the stored date/time of creation or modification of a file. (Haber and Stonetta (1991))

2.5.1.1.2 TIME STAMPING SCHEMES

There are many time-stamping schemes with different security goals, and these schemes are:

- (Public Key Infrastructure) PKI-based - Timestamp token is protected using PKI digital signature.
- Linking-based schemes - timestamps is generated such a way that it is related to other timestamps.
- Distributed schemes - timestamp is generated in cooperation of multiple parties.
- Transient key scheme - variant of PKI with short-living signing keys.
- MAC - simple secret key based scheme, found in ANSI ASC X9.95 Standard.
- Database - Document hashes are stored in trusted archive; there is online lookup service for verification. (Bonnecaze, A., Liardet, P., Gabillon, A., & Blibech, K. (2006, June))

The most common type of time-stamping technique used in the PKI-based Timestamp. The technique is based on digital signatures and hash functions. First a hash is calculated from the data. A hash is a sort of digital fingerprint of the original data: a string of bits that is different for each set of data. If the original data is changed, then this will result in a completely different hash. This hash is sent to the TSA. The TSA concatenates a timestamp to the hash and calculates the hash of this concatenation. This hash is in turn digitally signed with the private key of the TSA (Time Stamping Authority). This signed

hash + the timestamp is sent back to the requester of the timestamp who stores these with the original data. Since the original data cannot be calculated from the hash (because the hash function is a one way function), the TSA never gets to see the original data, which allows the use of this method for confidential data. (Bonnecaze, A., Liardet, P., Gabillon, A., & Blibech, K. (2006, June))

2.5.1.1.3 CHECKING THE TIMESTAMP

Checking correctness of a timestamp generated by a time stamping authority (TSA). Anyone trusting the time-stamper can then verify that the document was not created after the date that the time-stamper vouches. It can also no longer be repudiated that the requester of the timestamp was in possession of the original data at the time given by the timestamp. The hash of the original data is calculated, the timestamp given by the TSA is appended to it and the hash of the result of this concatenation is calculated, call this hash A. Then the digital signature of the TSA needs to be validated. This can be done by checking that the signed hash provided by the TSA was indeed signed with their private key by digital signature verification. The hash A is compared with the hash B inside the signed TSA message to confirm they are equal, proving that the timestamp and message is unaltered and was issued by the TSA. If not, then either the timestamp was altered or the timestamp was not issued by the TSA. . (Bonnecaze, A., Liardet, P., Gabillon, A., & Blibech, K. (2006, June))

2.5.1.2 DIGITAL SIGNATURES

A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that a known sender created the message, and that it is not altered in transit. The purpose of digital signature support is to provide a means to prevent anyone or anything from tampering with the contents of a business message, especially when the business message is in transit between two trading partners. A digital signature itself is a set of data appended to a business message consisting of an encrypted, one-way hash value of data packaged in a specific format (for example, PKCS7 Signed Data). (Merkle, R. C. (1990, January))

A digital signature:

- Validates that the contents of a digitally signed message have not been tampered with.
- Contains the identity of the sender of the business message.

The data required to create a digital signature is obtained from the trading partner configuration data in the repository. The information required to create a digital signature also includes the following:

- Trading partner signature certificate and private key
- Certificate authority certificate for the trading partner signature certificate
- Hash algorithm name: SHA1 and Signature algorithm name: RSA

2.5.1.3. TRUSTED THIRD PARTIES (TTP)

Trusted third parties may be involved in the provision of non-repudiation services, depending on the mechanisms used and the non-repudiation policy in force. The use of asymmetric cryptographic techniques requires authentic public keys which can be provided by certificates issued by third parties, e.g. by certification authorities. The use of symmetric cryptographic techniques requires the involvement of an on-line trusted third party to generate and verify secure envelopes (SENV). The non-repudiation policy in force may require evidence to be generated partly or totally by a trusted third party.

Trusted third parties may be involved to differing degrees in the phases of non-repudiation. When exchanging evidence, the parties shall know, be informed, or agree as to which non-repudiation policy is to be applicable to the evidence? There may be a number of trusted third parties involved acting in various roles (e.g., notary, time-stamping, monitoring, key certification, signature generation, signature verification, secure envelope generation, secure envelope verification, token generation, or delivery roles), as dictated by the non-repudiation policy. A single trusted third party might act in one or more of these roles. Examples of TTP are like banks, credit card companies, Internet service providers and mobile network operators. (Wikipedia, trusted third parties)

2.5.1.4. SECURE AUDIT LOG

This log typically stores each business message with its digital signature and secured timestamp. You use an audit log to reconstruct the sequence of messages and other

system events that have occurred during the exchange of business messages among trading partners.

For non-repudiation it is highly recommended that a developer incorporates either of the named mechanisms together to ensure a robust non-repudiation feature in the application.

But the most important of the above mentioned services for non-repudiation, the Non-repudiation of Origin (NRO) and Non-repudiation of Receive (NRR) are the most important mechanisms that any m-payment application should vigorously consider in the development.

2.5.2 Categories Of Non-Repudiation:

Non-repudiation service can be separated into non-repudiation of origin (NRO), non-repudiation of submission (NRS), non-repudiation of transport (NRT), and non-repudiation of delivery (NRD).

NRO is a combination of non-repudiation of creation and non-repudiation of sending, and NRD must be seen as catenation of non-repudiation of receipt (NRR) and non-repudiation of knowledge services are explained below (ISO/IEC13888-1: 2009: General Introduction):

2.5.2.1 Non-Repudiation of Origin (NRO)

The NRO service provides the recipient of data with proof that protects against any attempt by the sender to falsely deny sending the data. The evidence (non-repudiation of origin token, NROT) is generated by the originator of the message and sent to the

intended recipient. The originator sends both the message and the NROT to the recipient. To provide proof, the identities and the integrity of data must be confirmed, and the time stamps must be within the given time window.

2.5.2.2 Non-Repudiation of Receipt (NRR)

The NRR service provides the sender of data with proof that protects against any attempt by the recipient to falsely deny having received the data. The evidence (non-repudiation of receipt token, NRRT) is generated by the recipient of the message and sent to the originator.

The recipient sends both the reply message (if any) and the NRRT to the originator. To provide proof, the identities and the integrity of data must be confirmed, and the time stamps must be within the given time window.

2.5.2.3 Non-Repudiation of Submission (NRS)

The NRS service provides the sender of data (that may be another DA) with proof that protects against any attempt by the DA to falsely deny having accepted the data for transmission. The DA *does not care* what the content of the message is. The originator (or a preceding DA) has sent a message to the (next) DA that receives this message and sends the NRS token to the originator (or the preceding DA establishing a chain of intermediate NRST tokens providing chained NRS).

To provide proof, the identities and the integrity of data must be confirmed, and the time stamps must be within the given time window.

2.5.2.4 Non-Repudiation of Transport (NRT)

The NRT service provides the sender of data with proof that protects against any attempt by the DA to falsely deny having delivered the data to the intended recipient. The DA *does not care* what the content of the message is and *cannot guarantee* that the message is duly received by the recipient. The evidence (Non-Repudiation of transport token, NRTT) is generated by the DA delivering the message to the intended recipient (the last DA in the chain of DAs) and send back to the originator. To provide proof, the identities and the integrity of data must be confirmed, and the time stamps must be within the given time window.

The non-repudiation service involves the generation, verification and recording of evidence, and the subsequent retrieval and re-verification of this evidence in order to resolve disputes. Some non-repudiation services may be provided by grouping other services; for example: non-repudiation of origin can be provided by combining non-repudiation of creation and non-repudiation of sending, and non-repudiation of delivery can be provided by combining non-repudiation of receipt and non-repudiation of knowledge.

2.5.3 Mechanisms For Providing Non-Repudiation

Non-repudiation mechanisms providing evidence should be based upon cryptographic techniques using symmetric or asymmetric techniques as described by ISO/IEC13888-2:2009 or ISO/IEC13888-3: 2009, respectively.

Asymmetric encryption technique involves the use of two or more distinct keys for encryption and decryption purposes. This technique removes the risk of sharing keys to encrypt and decrypt data that is being posed by symmetric technique. The encryption key and decryption key are different hence the need to involve an off-line TTP (Trusted third parties) to guarantee the genuineness of keys (public key certificates management including CRLs and directory servers).

Symmetric encryption technique is an encryption technique whereby one key is used for both encryption and decryption purposes. Symmetric techniques (using secure envelopes) can be applied and it requires an on-line TTP for generation and validation of the secure envelopes including resolution of origin preventing fraudulent repudiation (mechanisms using shared secret keys does not allow a distinction to be made between the parties sharing the key, and thus – in contrast to digital signatures – does not provide NRO). The mechanisms have to provide protocols for the exchange of Non-Repudiation tokens specific to each kind of non-repudiation. These tokens may be stored as information by disputing parties for arbitration. (ISO/IEC13888-2:2009: Security techniques- Non-Repudiation- Using symmetric techniques)

The non-repudiation service involves the generation, verification and recording of evidence, and the subsequent retrieval and re-verification of this evidence in order to resolve disputes. For evidence generation, the TTP may act on behalf of a principal involved in as token generation authority (TGA), digital signature generating authority (DSGA), time stamping authority (TSA), notary authority (NA), and monitoring

authority (MA). Evidence transfer MAY be carried out by a TTP acting as delivery authority (DA) or evidence record-keeping authority (ERA). At last, the TTP may be in the role of an evidence verification authority (EVA). The above is based on the use of asymmetric techniques of non-repudiation.

(ISO/IEC13888-3:2009: Security techniques- Non-Repudiation- Using asymmetric techniques)

2.6 Development Platforms For M-Payment Application Development

Development platforms for mobile payment applications depend on the two standards being used by mobile phones today. The two standards are GSM and CDMA, thus the platforms needed to develop these applications must be able to support the functionality provided by these two standards. Mobile application development is the process by which application software is developed for small low-power handheld devices such as personal digital assistants, enterprise digital assistants or mobile phones. These applications are either pre-installed on phones during manufacture, or downloaded by customers from various mobile software distribution platforms.

2.6.1 C # (Sharp)

C# (pronounced *see sharp*) is a multi-paradigm programming language encompassing strong typing, imperative, declarative, functional, generic, object-oriented (class-based), and component-oriented programming disciplines. It was developed by Microsoft within its .NET initiative and later approved as a standard by Ecma (ECMA-334) and ISO (ISO/IEC 23270:2006). (Gavalas, D., & Economou, D. (2011))

2.6.2 Java

It is the most commonly used programming language to develop mobile based applications. Its founding logic is the use of classes and objects in the construction of the program. Established tools in java used in developing mobile payment applications an example is like the Java Platform, Micro Edition or Java ME. It is a Java platform designed for embedded systems (mobile devices are one kind of such systems) . Target devices range from industrial controls to mobile phones (especially feature phones) and set-top boxes. Java ME was formerly known as Java 2 Platform, Micro Edition (J2ME). Java ME was designed by Sun Microsystems, now a subsidiary of Oracle Corporation; the platform replaced a similar technology, Personal Java. Originally developed under the Java Community Process as JSR 68, the different flavors of Java ME have evolved in separate JSRs. Sun provides a reference implementation of the specification, but has tended not to provide free binary implementations of its Java ME runtime environment for mobile devices, rather relying on third parties to provide their own. (Kastner, C., Thum, T., Saake, G., Feigenspan, J., Leich, T., Wielgorz, F., & Apel, S. (2009))

2.6.3 C++ Language

The language is used to develop CDMA phone based applications. The Brew (Brew MP, Binary Runtime Environment for Wireless): is an application development platform created by Qualcomm, originally for CDMA mobile phones, featuring third party applications such as mobile games. It is offered in some feature phones but not in smart phones. It debuted in September 2001. As a software platform that can download and

run small programs for playing games, sending messages, and sharing photos, the main advantage of Brew MP is that the application developers can easily port their applications among all Brew MP devices by providing a standardized set of application programming interfaces. Software for the Brew MP enabled handsets can be developed in C or C++ using the freely downloadable Brew MP SDK (software development key). The Brew runtime library is part of the wireless device on-chip firmware or operating system in order to allow programmers to develop applications without needing to code for system interface or understand wireless applications. Brew is described as a pseudo operating system, but not a true mobile operating system. Brew is not a virtual machine such as Java ME, but runs native code. (Chen, B., Cheng, H. H., & Palen, J. (2006))

2.7 Existing Mobile Payment Applications

2.7.1 Mpesa

It is the product name of a mobile-phone based money transfer service for Safaricom, which is a mobile service provider. M-Pesa was initially developed by Sagentia before transitioning to IBM. The system was developed and ran by Sagentia from initial development to the 6 million customer mark. The pilot project was jointly funded by the UK government Department for International Development (DFID) and Vodafone's Kenyan affiliate Safaricom in 2003–2006 and commercially launched in 2007. (Mas, I., & Morawczynski, O. (2009))

The pilot was first used to disburse loans from Faulu (a Kenyan microfinance agency) to its clients and collect repayments. Additionally clients could deposit and withdraw cash

from authorized M-PESA agents, make person-to-person (P2P) money transfers, purchase airtime for re-sale or personal use.

The service has now been transitioned to be operationally run by IBM Global Services on behalf of Vodafone. The initial 3 markets (Kenya, Tanzania & Afghanistan) are hosted between Rackspace and Vodafone.

M-Pesa customers can deposit and withdraw money from a network of agents that includes airtime resellers and retail outlets acting as banking agents. M-Pesa is operated by Safaricom, a mobile network operator (MNO), which is not classed as a deposit-taking institution (such as a bank). Therefore, M-Pesa may not be advertised as a banking service.

The service enables its users to:

- Deposit and withdraw money
- Transfer money to other users and non-users
- Pay bills and also to purchase airtime

The user interface technology of M-Pesa differs between Safaricom of Kenya and Vodacom of Tanzania, although the underlying platform is the same. While Safaricom uses SIM toolkit to provide handset menus for accessing the service, Vodacom relies on USSD to provide users with menus.

Concept of Mpesa

The initial concept of M-Pesa was to create a service which allowed microfinance borrowers to conveniently receive and repay loans using the network of Safaricom airtime resellers. This would enable microfinance institutions (MFIs) to offer more competitive loan rates to their users, as there is a reduced cost of dealing in cash. The users of the service would gain through being able to track their finances more easily. But when the service was trialed, customers adopted the service for a variety of alternative uses and complications arose with Faulu, the partnering MFI. M-Pesa was re-focused and launched with a different value proposition: sending remittances home across the country and making payments. (Hughes, N., & Lonie, S. (2007)

M-Pesa is a branchless banking service, meaning that it is designed to enable users to complete basic banking transactions without the need to visit a bank branch. The continuing success of M-Pesa in Kenya has been due to the creation of a highly popular, affordable payment service with only limited involvement of a bank.

2.7.2 Paybox

One of the most widespread mobile phone payment applications is Paybox (Paybox.net, 2002), which was launched in Germany in May 2000. Later it was launched in Austria, Spain, Sweden and the UK. This service enables customers to purchase goods and services and make bank transactions via mobile phone. The value of purchases or credit transfers is debited from customers' bank account. The infrastructures needed to use Paybox are a mobile phone, a bank account and a Paybox registration. Customers send their phone number to a merchant. The merchant communicates this phone number and

the price. The Paybox system calls the customer and asks for payment authorization. Payers authorize by their PIN. Paybox informs the trusted third party to settle the payment.

The disadvantages are that the operation of Paybox is expensive since the system has to make voice calls using integrated voice recognition system (IVR) to the customer, which could range over various durations. In addition, there is no data privacy and customer and merchant have no proof of transaction, which might be a possible cause of fraud. The high latency also restricts it to high value transactions (Fischer, 2002). Most of all the transaction can be done only using a GSM enabled phone.

A typical real-world Mobile transaction flow chart using Paybox is given in the Figure 2.7.2 on the next page.

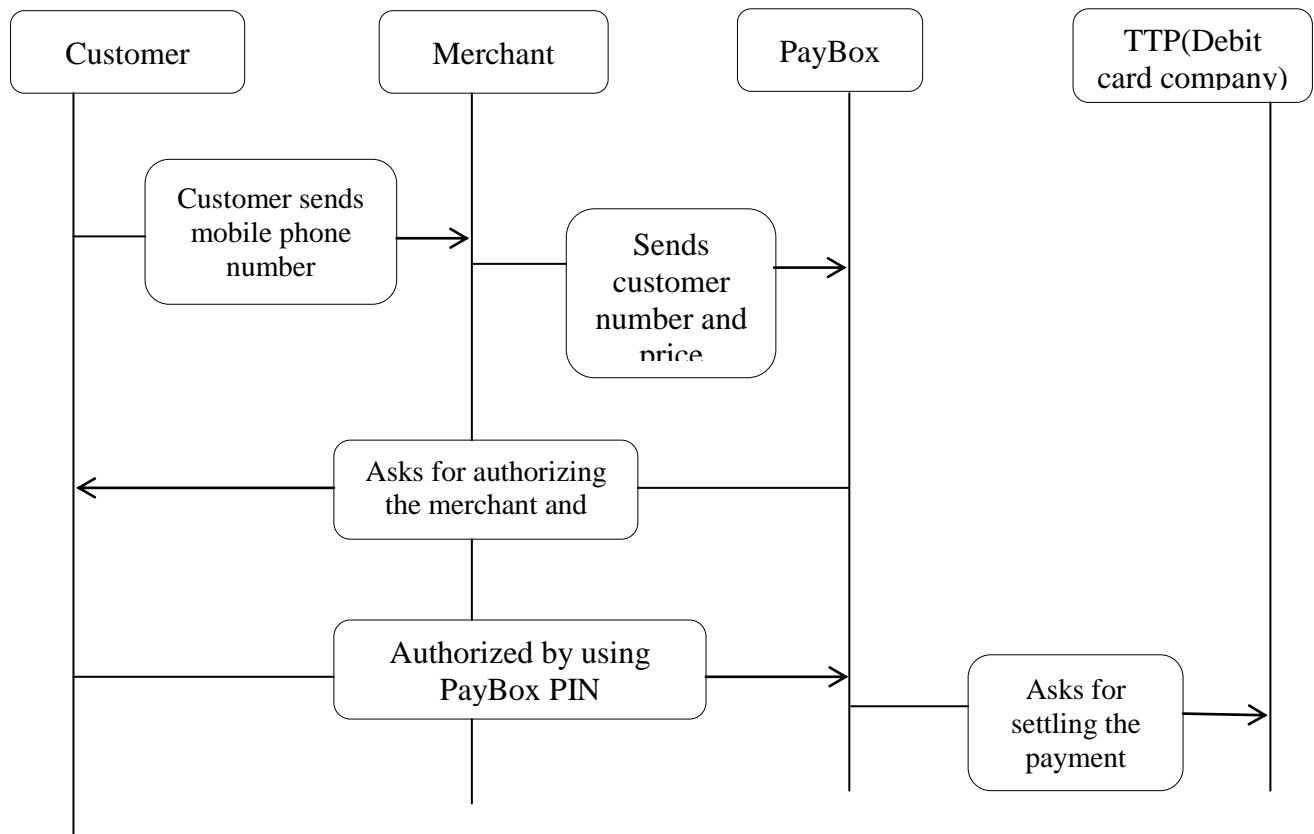


Figure 2.7.2: Pay box mobile transaction model

2.7.3 M-Pay

M-Pay is a mobile payment solution developed in corporation PBS, Orange and Gem plus. It is a server-based credit/debit card payment solution via mobile phone for goods ordered via telephone sales and on the Internet through the PC or a WAP mobile phone. To use this application the user sends a written application to Orange asking to link the payment data to the GSM data in a payment server. Activating the payment function on the mobile phone requires an individually allocated PIN-code, which is connected to the SIM-card in the mobile phone. (Fischer, 2002) A typical transaction flow chart using m-Pay is given in the Figure 2.7.3 on the next page.

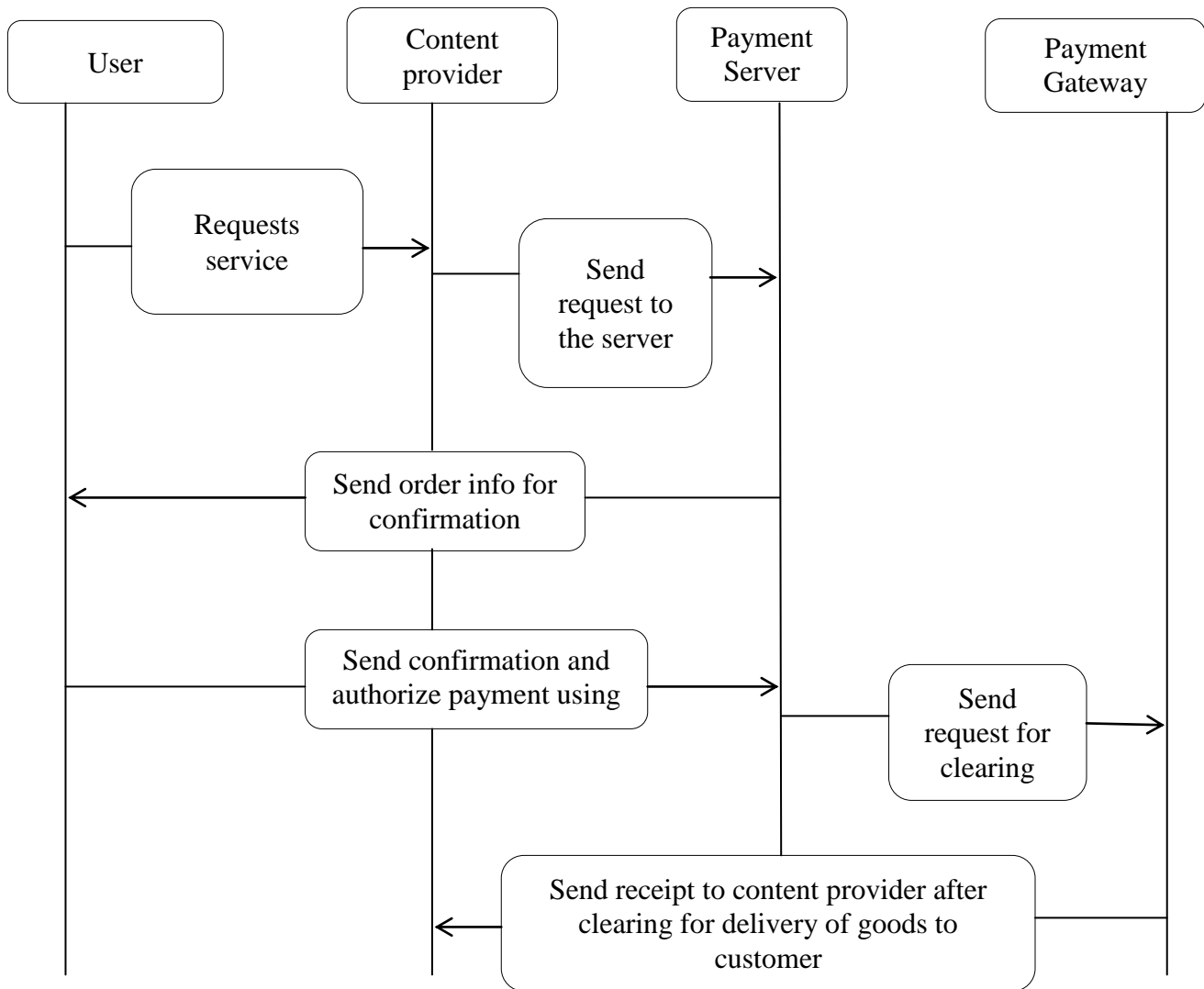


Figure 2.7.3: M-pay transaction model

Customers request a service or product from the content provider. This request in the form of an SMS message is sent to payment server, which takes care of authorizing the payment request. Payment server sends the order information to customers for confirmation, which customers do by using a personal identification number presented in the SIM card. The server will then translate the mobile phone number into a valid card

number and conduct a debit/credit card transaction. This confirmation is sent to the payment gateway for clearing, after which a receipt is generated by the gateway and sent to the content provider.

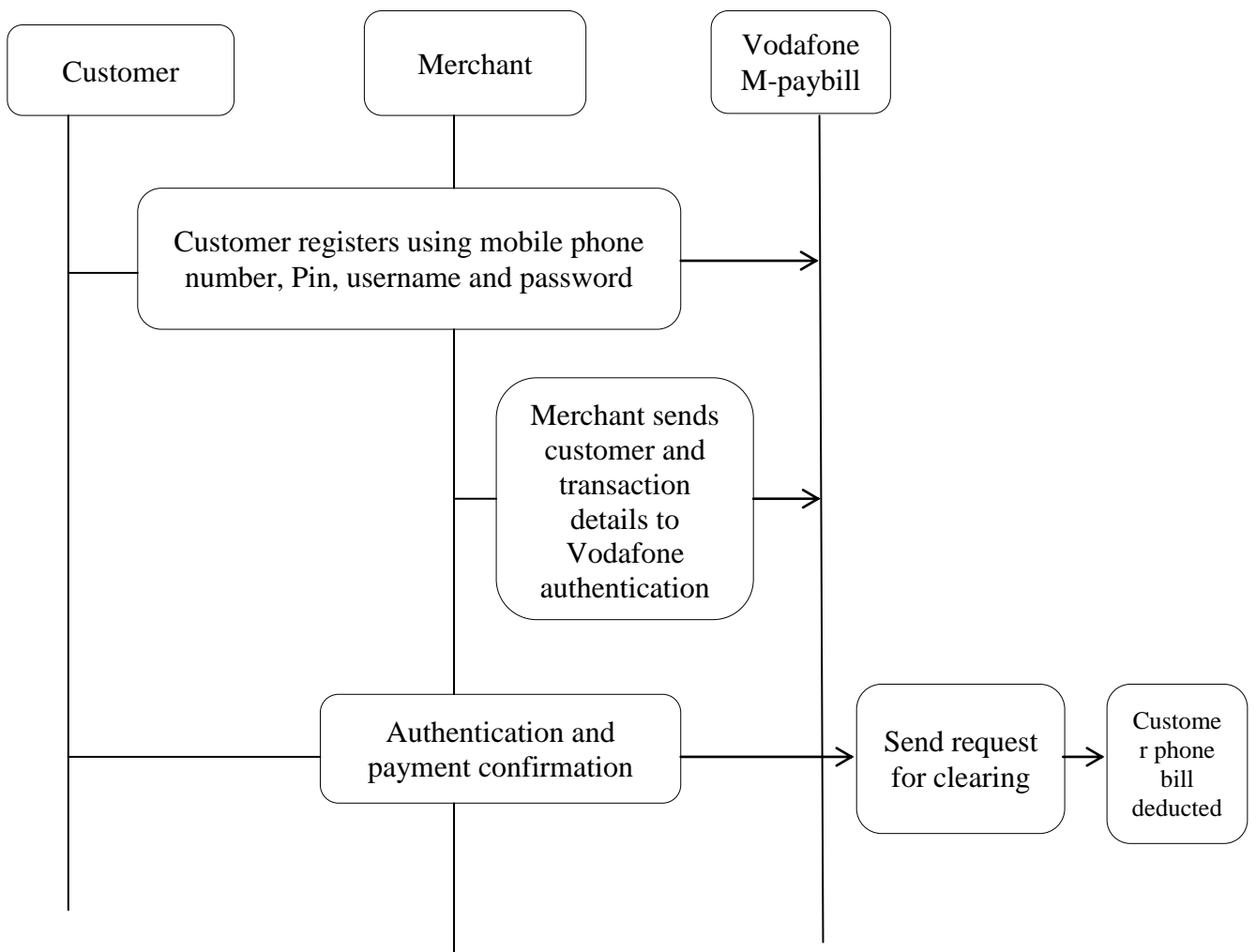
2.7.4 Vodafone M-Paybill

M-PayBill supports virtual Point of Sale (POS) for micro and small payments. The bill is charged to customers' phone bill or from the prepaid airtime. The requirements for this payment solution are a WAP phone or a Web browser to settle the payment. The Vodafone customers register for M-PayBill online by entering their mobile phone number, choosing a username, a password, and a four-digit PIN. When using a WAP phone the user is asked to enter the PIN for identification. Purchase amount is then charged to the phone bill or deducted from prepaid airtime.(Fischer, 2002)

M-PayBill membership is free; there are no basic or transaction fees. No extra infrastructure needed to perform the transaction except for a WAP phone. M-PayBill provides interoperability by having service providers outside of European Union plus Norway, Iceland and Liechtenstein. The personal information is transferred to the service providers in other countries for purchases outside the European Union. The security of the information will then depend on the privacy policy of that country. Payment information is maintained on the server and does not change hands, thus preventing any chances of fraud. The process is basically easy to understand and provides faster transactions. Customers already registered with the Vodafone network

operator need not register again to use the procedure. Payment solution, however, is only applicable to micro-payments. Figure 2.7.4 shows a typical micro payment transaction using Vodafone

Figure 2.7.4: Vodafone m-PayBill transaction model



2.8 Conclusion

From the literature review the following aspects were noted,

First most mobile payment applications use the Personal Identification Number mechanisms to authorize transactions in their applications because it is easy to implement and it does not cost that much to implement the PIN mechanism. Other authorization mechanisms like biometric authorization would require additional devices like biometric readers or scanners to get the biometric information from the users and thus the cost of implementing such an authorization mechanism in the application would greatly increase the cost of implementing or developing the application. While on the other hand most mobile payment applications in Kenya do not use digital signatures because they are a bit costly to implement in such a scenario. Thus from the literature review, I settled down on the PIN mechanism due to the fact that it would not be expensive and it is easy to implement.

Another aspect that was noted from the literature review is that most PIN algorithms do not cater for the implementation of non-repudiation in their algorithm. The PIN algorithms like the IBM and VISA PIN algorithms all don't cater for non-repudiation provision in their algorithms.

Also most mobile payment applications that were looked at in the literature review provided for non-repudiation services only at the transaction initiation level. Most did not cater for non-repudiation from the authorization level but only at the transaction initiation level. Hence the project sought to address this issue by ensuring that

transactions are initiated right from the authorization point and not only at the transaction ignition phase.

Another aspect from the literature review is the choice in the use of timestamps to implement together with PIN to enhance non-repudiation. The reason being timestamps actually show the time a certain event took place, in this case the time a transaction was effected between the parties involved. Thus with timestamps the aspect of non-repudiation would be taken care of when it came to implementation of the proposed application, while for authorization using PIN would also suffice.

The above literature review impacted on my proposed approach because I settled on the two mechanisms PIN and timestamps because:

1. They are easy to implement
2. They are cost effective

And thus would use the timestamp mechanism to enhance non-repudiation provision capabilities of the PIN mechanism. In the light of this, the two mechanisms were to be implemented together and provide non-repudiation in mobile payment applications from authorization point of the application.

CHAPTER THREE

METHODOLOGY

3.0 Introduction

The purpose of this section of the thesis helped in coming up with the requirements specification for the proposed application through data collection and analysis. The results of this chapter were used in coming up with the design of the mobile payment application. This chapter consists of the methodology used, research design, target population, sampling techniques, the data collection tools.

3.1. Waterfall Methodology

The **waterfall model** is a sequential software development process, in which progress is seen as flowing steadily downwards (like a waterfall) through the phases of Conception, Initiation, Analysis, Design (validation), Construction, Testing and maintenance.

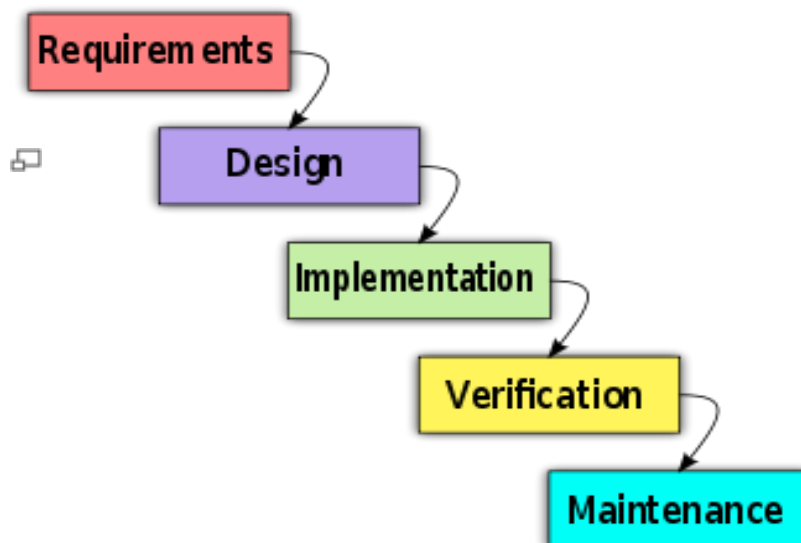


Figure 3.1: Waterfall model

The waterfall development model has its origins in the manufacturing and construction industries; highly structured physical environments in which after-the-fact changes are prohibitively costly, if not impossible. Since no formal software development methodologies existed at the time, this hardware-oriented model was simply adapted for software development.

The first formal description of the waterfall model is often cited to be an article published in 1970 by Winston W. Royce (1929–1995), although Royce did not use the term "waterfall" in this article. Royce was presenting this model as an example of a flawed, non-working model (Royce 1970). This is in fact the way the term has generally been used in writing about software development—as a way to criticize a commonly used software practice.

The stages of "The Waterfall Model" are:

Requirement Analysis & Definition: All possible requirements of the system to be developed are captured in this phase. Requirements are set of functionalities and constraints that the end-user (who will be using the system) expects from the system. The requirements are gathered from the end-user by consultation, these requirements are analyzed for their validity and the possibility of incorporating the requirements in the system to be development is also studied. Finally, a Requirement Specification document is created which serves the purpose of guideline for the next phase of the model.

System & Software Design: Before a starting for actual coding, it is highly important to understand what we are going to create and what it should look like? The requirement specifications from first phase are studied in this phase and system design is prepared. System Design helps in specifying hardware and system requirements and also helps in defining overall system architecture. The system design specifications serve as input for the next phase of the model.

Implementation & Unit Testing: On receiving system design documents, the work is divided in modules/units and actual coding is started. The system is first developed in small programs called units, which are integrated in the next phase. Each unit is developed and tested for its functionality; this is referred to as Unit Testing. Unit testing mainly verifies if the modules/units meet their specifications.

Integration & System Testing: As specified above, the system is first divided in units that are developed and tested for their functionalities. These units are integrated into a complete system during Integration phase and tested to check if all modules/units coordinate between each other and the system as a whole behaves as per the specifications. After successfully testing the software, it is delivered to the customer.

Operations & Maintenance: This phase of "The Waterfall Model" is virtually never ending phase (Very long). Generally, problems with the system developed (which are not found during the development life cycle) come up after its practical use starts, so the issues related to the system are solved after deployment of the system. Not all the problems come in picture directly but they arise time to time and needs to be solved; hence this process is referred as Maintenance.

Demerits of the model

- 1) As it is very important to gather all possible requirements during the Requirement Gathering and Analysis phase in order to properly design the system, not all requirements are received at once, the requirements from customer goes on getting added to the list even after the end of "Requirement Gathering and Analysis" phase, this affects the system development process and its success in negative aspects.
- 2) The project is not partitioned in phases in flexible way.
- 3) As the requirements of the customer goes on getting added to the list, not all the requirements are fulfilled, this results in development of almost unusable system. These requirements are then met in newer version of the system; this increases the cost of system development.
- 4) The greatest disadvantage of the waterfall model is that until the final stage of the development cycle is complete, a working model of the software does not lie in the hands of the client. Thus, he is hardly in a position to mention if what has been designed is exactly what he had asked for.

Advantages of the Waterfall Model

1. It is a linear model and of course, linear models are the most simple to be implemented.
2. The amount of resources required to implement this model is very minimal.
3. One great advantage of the waterfall model is that documentation is produced at every stage of the waterfall model development. This makes the understanding of the product designing procedure simpler.

4. After every major stage of software coding, testing is done to check the correct running of the code.

3.1.1 Why Choice In The Waterfall Model

This model was chosen due the fact that the requirements that were gotten from the analysis part were well understood and unlikely to change during the course of even doing the design of the proposed solution. This model makes it possible for the outcome in the previous stage to be used in the next stage and due to the nature of resource and time constraints involved in the project it was the best placed model to use in the requirements specification, design and modeling of the proposed solution.

3.2 Research Design

The research design that shall be used in this project is the surveys. The reason for the use of survey design is that it will help me the researcher to choose a target sample from the overall population that shall be used in the research and that is managers/ business owners and thus will help me in sticking to my target population and not to overstep the boundaries.

3.3 Target Population

The characteristic of the population

- Owners/proprietors of small and medium sized businesses involved in m-commerce or have used mobile payment to do a transaction. They are relevant to the study because they own the businesses or manage them and have insight into the research area.

- Mobile service providers: they provide mechanism for authorizing and ensuring non-repudiation of transactions, and they provide a platform where these applications operate on.

3.4 Sample Size And Procedures

The sample size for the project will consist of 50. The purposive sampling will be used because it will allow me (The researcher) to use cases that have the required information with respect to this project. Thus 47 SME will be considered and 3 Mobile service operators/providers.

3.5 Data Collection And Data Analysis

As a researcher the first part one does even before formulating what data collection tools and procedures they will use they must come up with a research design. The research design used in this research project was that of surveys. The main reason for using surveys was that it helps the researcher to stick only to the sample population that has the required information. The sampling procedure used was the purposive sampling that falls under the non-probability sampling. Reason for using the stated sampling technique is that this technique allows the researcher to use cases that have the required information with respect to the objective of the study they are carrying out. The sample was targeting business owners and mobile service providers. Thus with respect to both the two main sample targets, it was deemed necessary to have two different questionnaires for each of the established cases.

3.5.1 Data Collection Techniques

Data collection was based on two techniques that were used in this project. The first technique employed was that of doing the background reading based on similar or existing systems that have been done. This was very helpful especially in getting to know the way these systems were implemented, the tools used. This helped a lot in forming a basis for my literature review. Through this background reading it helped in already establishing the areas that were dealt with and not going over them again.

Questionnaires were also used in this section. They were used to get important information about the population. The research depended on this technique because of the time constraint associated with the research hence questionnaires were dispatched to the identified respondents who would fill them at their own time and return them. Also the questionnaires did not require the respondents to identify themselves hence gave the respondents the freedom to openly respond to the items in the questionnaire.

The questionnaire used employed both use of open ended and close ended questions. The closed-ended questions are easier to analyse since they are in an immediate usable form, easier to administer because each item is followed by alternative answers as well as being economical to use in terms of time and money (Mugenda & Mugenda, 2003). While the open ended questions in the questionnaire were designed in such a way to help the respondent to give a full and meaningful answer according to his/her own knowledge of the subject matter. The open ended questions, helped in knowing the respondents feelings towards the subject matter.

3.5.2 Data Analysis

Data obtained from the field is raw hence difficult to interpret and must be processed and analyzed for it to make sense for the researcher. According to Kothari (2004), the term analysis refers to the “*the computation of certain measures along with searching for patterns of relationships that exist among the data groups*”. Analysis for this research project was classified under the frequency distribution of the items. A frequency distribution gives a record of the number of times a score or a response occurs.

The main aim of this analysis was to answer the following objectives:

- Identifying the security challenges affecting mobile payment transactions.
- Knowing if the users awareness and perception of the various authorization and non-repudiation mechanisms in use today in the various applications.
- Knowing the various measures mobile network operators or the regulator is actually doing to try and curb the problem of repudiation.
- Knowing the percentage/number of the respondents who use mobile payment in their business
- Their experience meter that is what is their experience on use of these mobile payment applications.

Hence it was necessary for the items in the questionnaire to be grouped according to the objectives. Therefore the analysis that shall be presented shall also be in the order of the above objectives. The sample population for this project was 50 respondents, of these 47

were to be business owners and 3 of them to be mobile service providers. Of the 47 business respondents 40 answered their questionnaires ok and on time while 3 have not yet finalized on their questionnaire and 4 were spoilt questionnaires (the respondents didn't answer the questions correctly). Due to the time constraint the 40 questionnaires were analyzed based on the fact that more than half of the intended respondents had filled in the questionnaires correctly. For the mobile service providers, only one of them agreed to participate in the study, though they did not provide in full the technical details of their mobile payment service.

CHAPTER FOUR

ANALYSIS AND RESULTS

4.0 Introduction

The main aim of this analysis chapter was to answer the analysis objectives (3.5.2) which were stated in the methodology chapter.

4.1 Knowing The Percentage Of The Respondents Who Use Mobile Payment In Their Business.

Use mobile phone	Frequency	Percentage
Yes	24	60
No	16	40
Total	40	100

Table 4.1: Frequency distribution of the respondents who use mobile payment

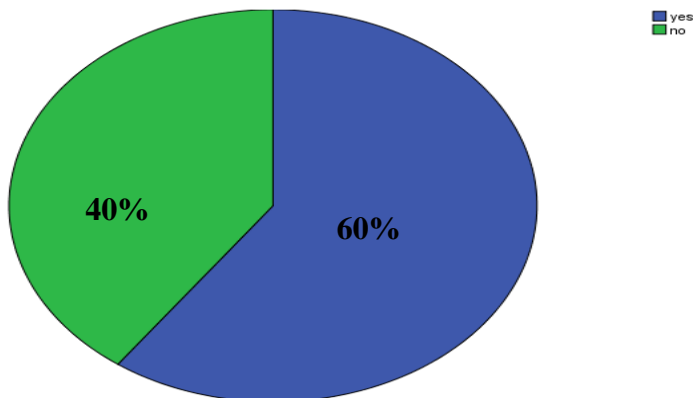


Figure 4.1: Pie chart for use of mobile payment applications in businesses

From the above pie chart figure 4.1, the study revealed that 60% percent of those interviewed used mobile payment in their businesses or agreed to do transactions through mobile payments systems while 40% didn't use it to do their transactions. The following statement below best describes the finding that a lot of people/business people actually agree to use mobile payment to do their transactions with their customers. We see that the number of mobile money subscriptions were 18.9 million. Quote from CCK (Sector statistics report Q2 2011/2012 Communications Commission of Kenya) "During the quarter under review, an increase of 3.08 per cent subscriptions in mobile money transfer was recorded from 18.4 million in the previous period to 18.9 million. Compared to the same period of the previous year, an increase of 42.13 per cent in mobile money subscriptions was registered. Moreover, the number of mobile money transfer subscriptions represents 70.35 per cent of the total mobile subscriptions. This rapid uptake of mobile money is an indication of the continued demand of the service particularly to low income earners who do not have access to banking services".

4.2 Age Distribution Of The Respondents

Age interval	Frequency	Percent
20-30	20	50%
31-40	14	35%
41-50	4	10%
51-60	2	2%

Table 4.2: frequency distribution for age

In table 4.2 on the previous page, the frequency distribution was highly used in giving the analysis for this research project, in the table we gave the age interval or divided the age into frequencies of 9 each. From the table we see that the respondents who were aged between 20 and 30 years of age were the most followed by those in their mid-30 and 40 respectively. Figure 4.2 below the pie chart for the above.

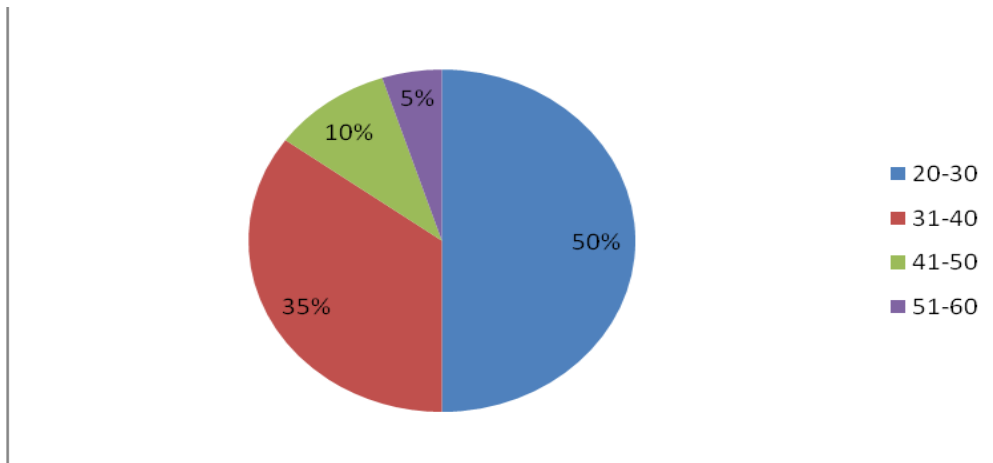


Figure 4.2: pie chart for age of the respondents

4.3 Education Level Of The Respondents

Education level	Frequency	Percent
Primary	9	22.5
Secondary	18	45.0
College/university	13	32.5
Total	40	100

Table 4.3: Education level of the respondents

Table 4.3 on the previous page shows the respondents education status. It shows clearly that most of the respondents attained secondary school education and while few of them only had primary education. This clearly is clearly depicted in figure 4.4 below whereby secondary education accounted for 45%, followed by university/college respondents who had 32.5% and lastly those who had primary education accounted for 22.5% of the respondents.

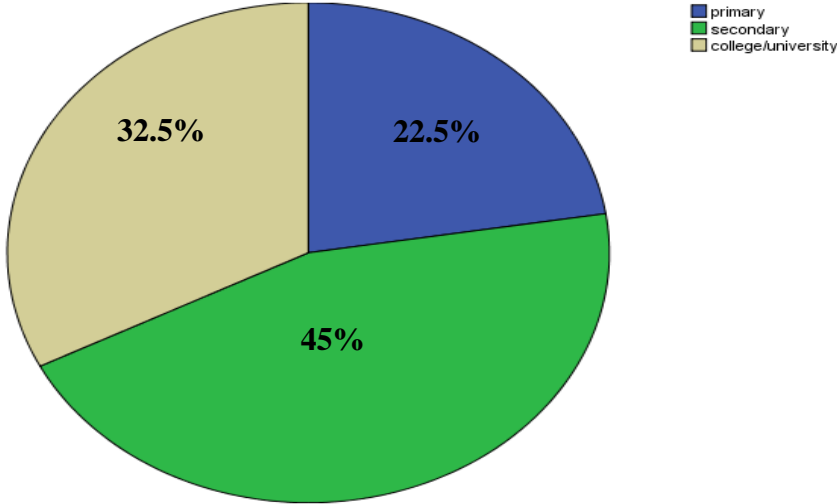


Figure 4.3: Chart for education level of the respondents

This analysis helped us in knowing the education level of the respondents. It will also help us as we progress through to find out if education status of the respondents actually influenced their choice of using mobile applications in their business and their perception towards how they felt about the security of these mobile payment applications and their authorization and non-repudiation mechanisms.

4.4 Respondents Experience In Using Mobile Payment

Experience of respondents to mobile payment use	Frequency	Percent
None	5	12.5
Novice	11	27.5
Advanced	24	60
Total	40	100

Table 4.4: frequency distribution of the experience level of the respondents

From the pie chart figure 4.4 below, we get the experience levels of respondents in using mobile payment applications, from the respondents we had 12.5% didn't have any experience on using mobile payment applications, 27.5% had but not that in depth while 60% had much knowledge in using mobile payment applications. From this we see that those respondents who didn't use mobile payment in their businesses still knew how to use mobile payment applications.

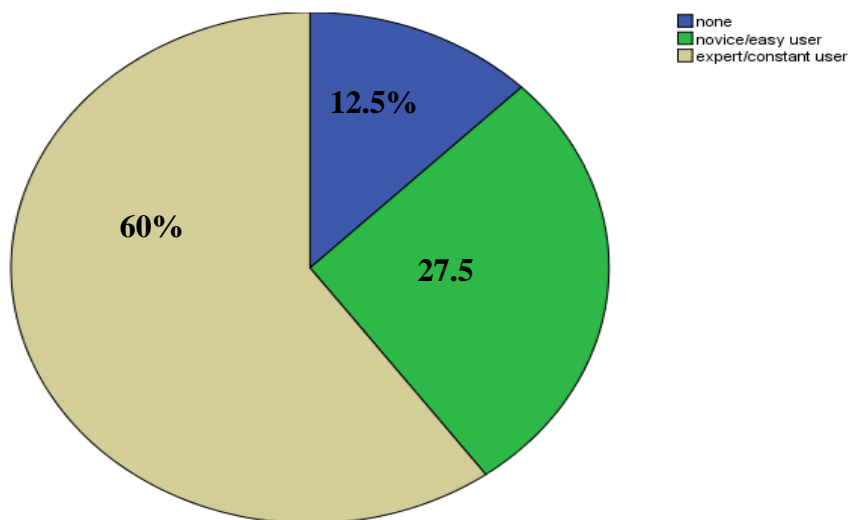


Figure 4.4: Pie chart for experience in using mobile payment applications

4.5 Gender Distribution Of The Respondents

Gender of respondents	Frequency	Percent
Male	18	45
Female	22	55
Total	40	100

Table 4.5: Gender of the respondents

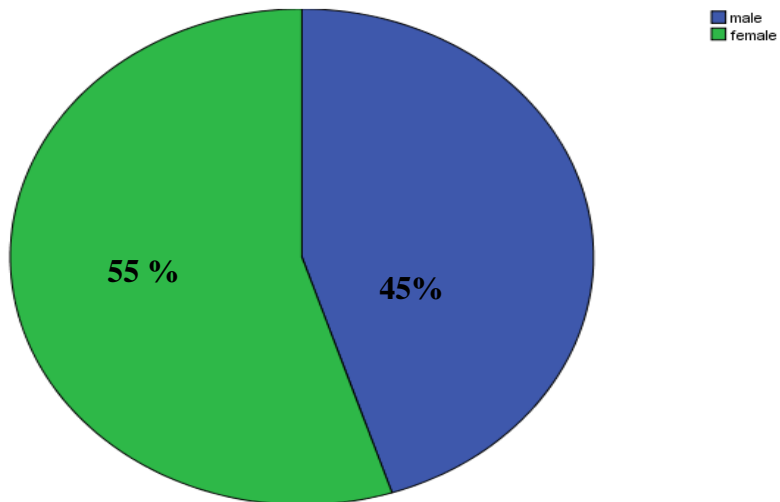


Figure 4.5: Pie chart depicting the percentages of the respondents involved in the study

From the above figure we see that most of the respondents were female who had a 55% involvement in the study while male were 45%. All the respondents in this study were involved in businesses in Thika town.

4.6 Respondents Knowledge Of Authorization And Non-Repudiation Mechanisms

Mechanism For authorization	Know	Don't know
PIN	36	4
Biometrics	24	16
Digital Signatures	20	20
Username and passwords	38	2

Table 4.6: user's response on their knowledge of authorization mechanisms

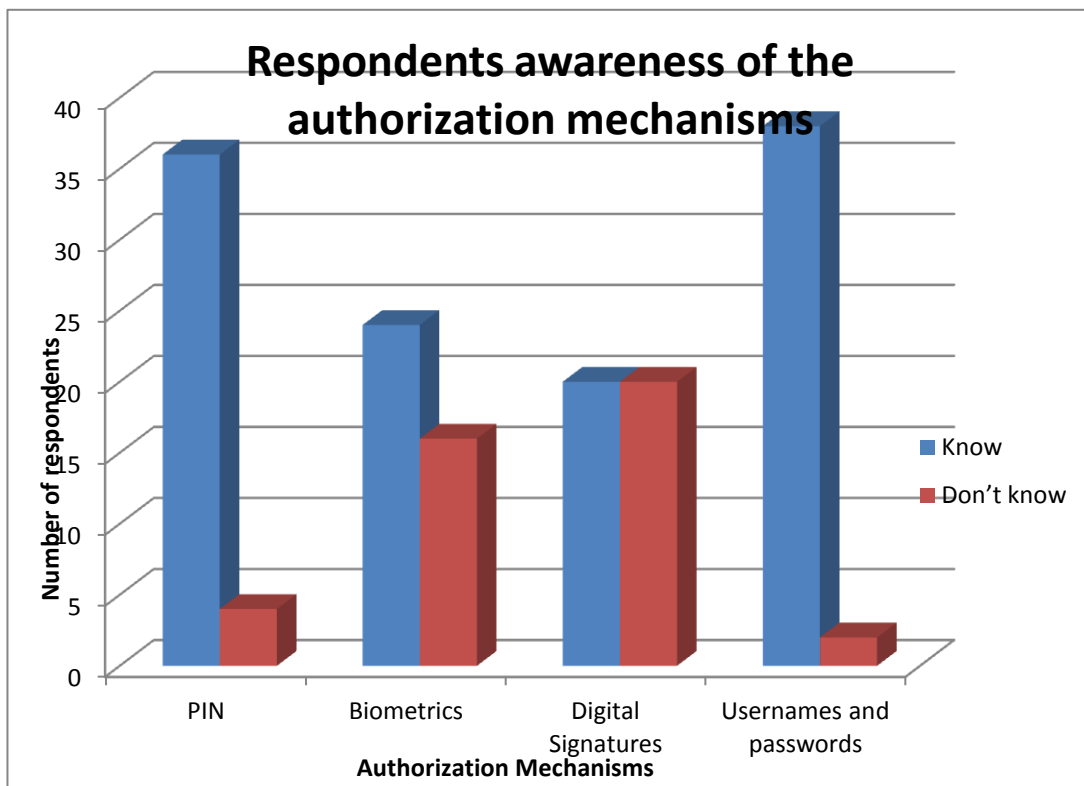


Figure 4.6: awareness to authorization mechanisms in use

Figure 4.6 in the previous page shows the user's knowledge on the given authorization mechanisms found in most mobile payment applications. Most of the respondents had

knowledge in the use of usernames and passwords followed by the use of the personal identification number mechanism. The least mechanism they knew about was the use of digital signatures where we find that the highest number of respondents did not know about this mechanism. So from the above graphs it shows clearly that the respondents know more about username accounts and personal identification number mechanism. The personal identification number has the highest frequency of users pertaining to know because it is evident in most of the mobile payment applications in use today it is the most used authorization mechanism. The reason for use of PIN is that it is unique to each user and it is difficult for a fraudster to know the PIN of a person if he/she keeps it safe.

Mechanisms for non-repudiation	Know	Don't know
Timestamps	32	8
Digital signatures	20	20
Secure logs	14	26

Table 4.6.1: Users response on their knowledge of non-repudiation mechanisms

Figure 4.6.1 in the next page shows the way the respondents answered the question on which non-repudiation mechanisms they knew. From the study it was seen that most of the respondents knew timestamps and digital signatures but most of them did not know on secure logs use in providing non-repudiation. It was noted that most of the respondents knew of the timestamp mechanism because most applications sent to them

the time at which a transaction had been effected. The timestamp mechanism has the highest number of respondents because most transactions in the current applications provide the time the transaction was effected between the two or more persons involved.

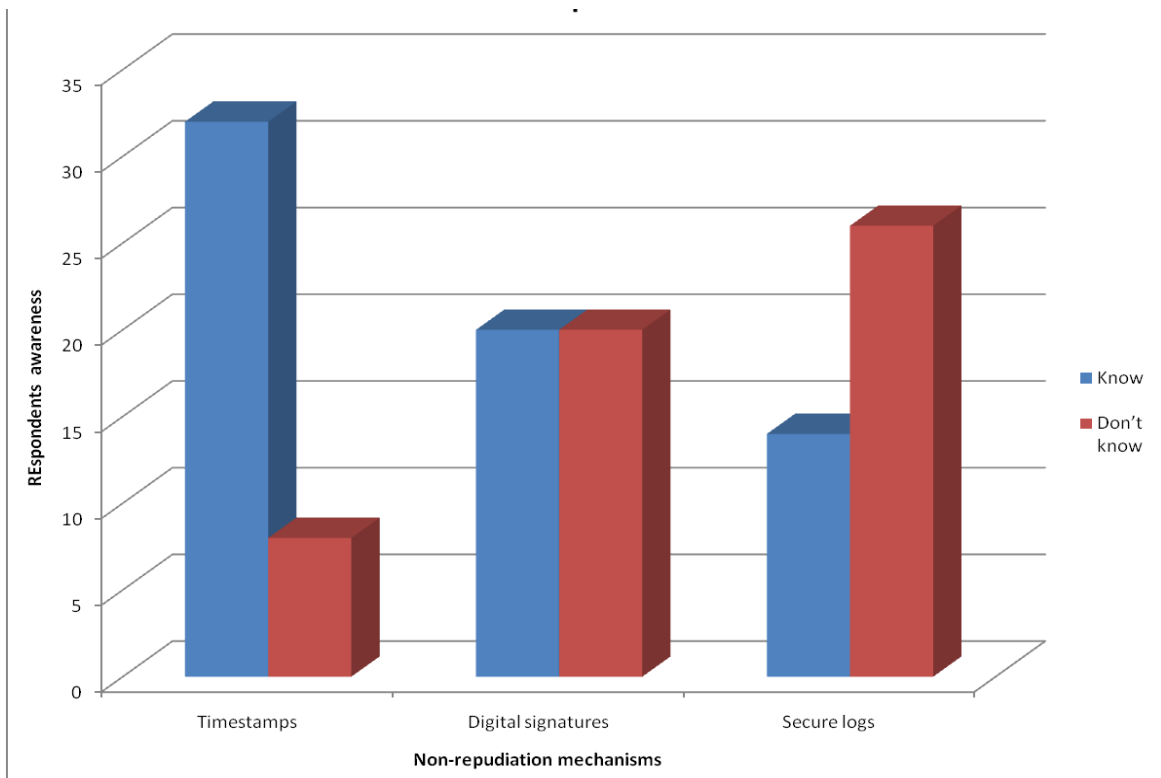


Figure 4.6.1: Awareness on non-repudiation mechanisms

The reason why the respondents were so much aware of the very deep IT security in both the authorization and non-repudiation mechanisms was because as I was doing the study most of my respondents were people who had access to other financial products being offered by financial institutions like banks and Sacco's hence had firsthand knowledge about these mechanisms. My target population for the study was business

owners thus most of them also access services offered by banks and Sacco's. Also change in curriculum whereby computer is taught in our schools is also a contributing factor where half of the respondents had secondary education and above that is as noted with the education level of the respondents, 13 of the respondents had university education while 28 had up to secondary education and also access to information on the internet whereby the respondents equally knew of mechanisms like the use of passwords and usernames which are the most common form of authentication in emails.

4.7 Security Challenges in Mobile Payment.

Challenge	Yes it affected Them	No it didn't affect them
Theft of PIN	19	21
Cancellation of a wrong transaction	18	22
Sending money to the wrong recipient	28	12
Mobile fraud	15	25

Table 4.7: Challenges facing mobile payment users

Table 4.7 above shows the way the respondents answered to the open question on which challenges they face while using mobile payment applications, from the above graph it shows that many of them noted down that sending money to the wrong recipient as being the hardest challenge they face, followed by theft of their secret PIN number. Also the respondents said that many mobile applications take long to cancel wrong transactions, in this case the problem/challenge of sending money to the wrong recipient led to the challenge of not being able to cancel that transaction in time before the person

withdrew the money. Also the respondents noted down the challenge of mobile fraud whereby fraudsters fraud you of your money. They claimed that most of these fraudsters send them messages purporting to be from the service provider telling them of a transaction they made yet they didn't and wanted a refund of the money.

Figure 4.7 below depicts this using a bar chart to show the security challenges the users face will transacting using mobile payment application

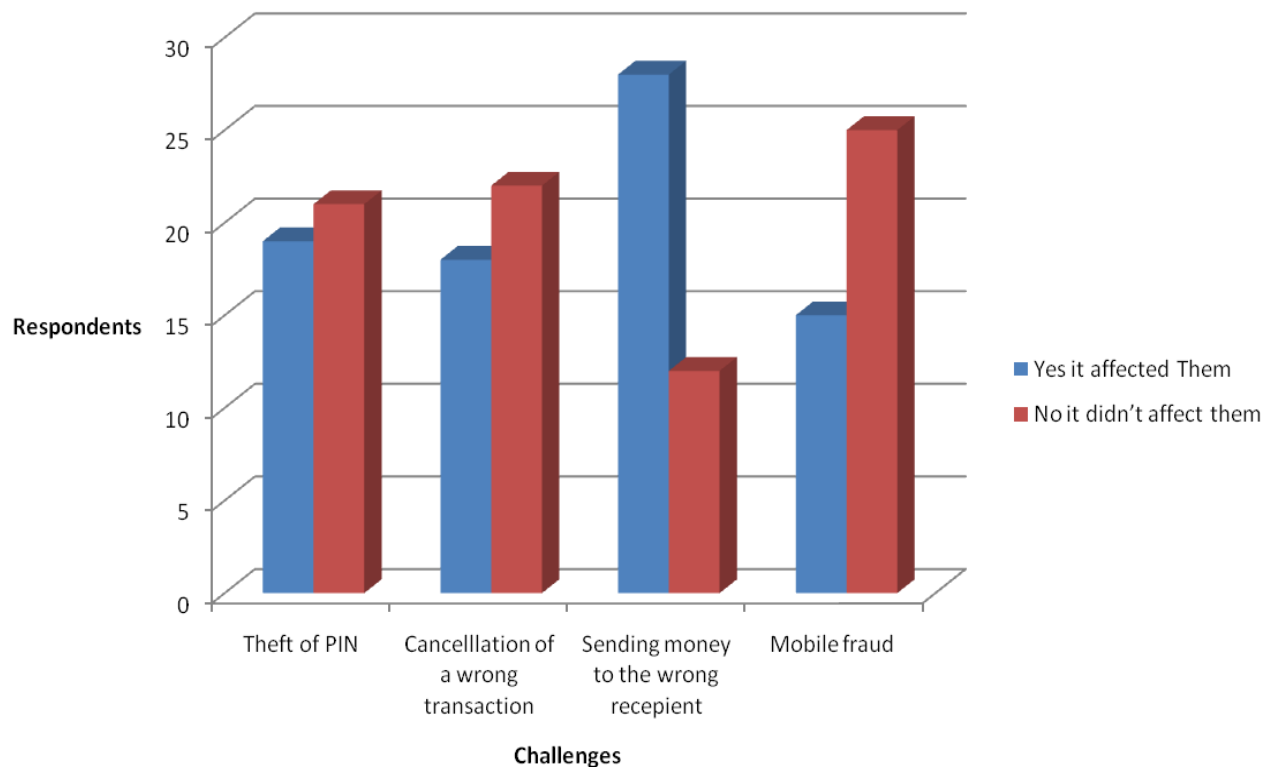


Figure 4.7: Mobile payment challenges facing users

4.8 Measures To Curb The Security Challenges By Mobile Service Providers

The mobile service provider pinpointed problems like PIN theft, Mobile fraud and sending money to the wrong recipient. Mobile fraud occurs in many forms, one of which

is sending of false transaction messages purporting to have made a transaction which has not been made to their victims who in turn fall into their ploy either to make a payment into their account or they default on their intended transaction.

The response from the mobile service provider that participated in this study revealed of intricate measures they undertake in case a repudiation case occurs. First they flag the suspected transactions, they bar the account involved in that transaction and then transfer the case to their internal fraud section to follow through with the local authorities.

4.9 Respondent's Attitude Towards Current Mobile Systems.

Table 4.9 on the next page shows how the respondents answered the question on how they would rate current mobile payment systems security. It shows clearly that a majority of the respondents liked/agreed that current mobile payment applications are safe. This is largely attributed to the security measure undertaken by the various mobile service providers on whose platforms these applications run to ensure that the security of the users is of their utmost concern.

Figure 4.9 on the next page shows a majority of those who use mobile payment and those who don't use mobile payment agree that current mobile payment applications are safe, but similarly those who agree to use still find it to be unsecure and many of them are neutral on the issue. This is mostly attributed to the measures the mobile service provider takes to tackle cases of mobile fraud or other challenges that may affect the users which ensures that most of these challenges are mitigated

Respondents attitude towards current mobile payment security	Frequency
Strongly Disagree	7
Disagree	8
Neutral	9
Agree	13
Strongly Agree	3
Total	40

Table 4.9: Respondent's attitude response

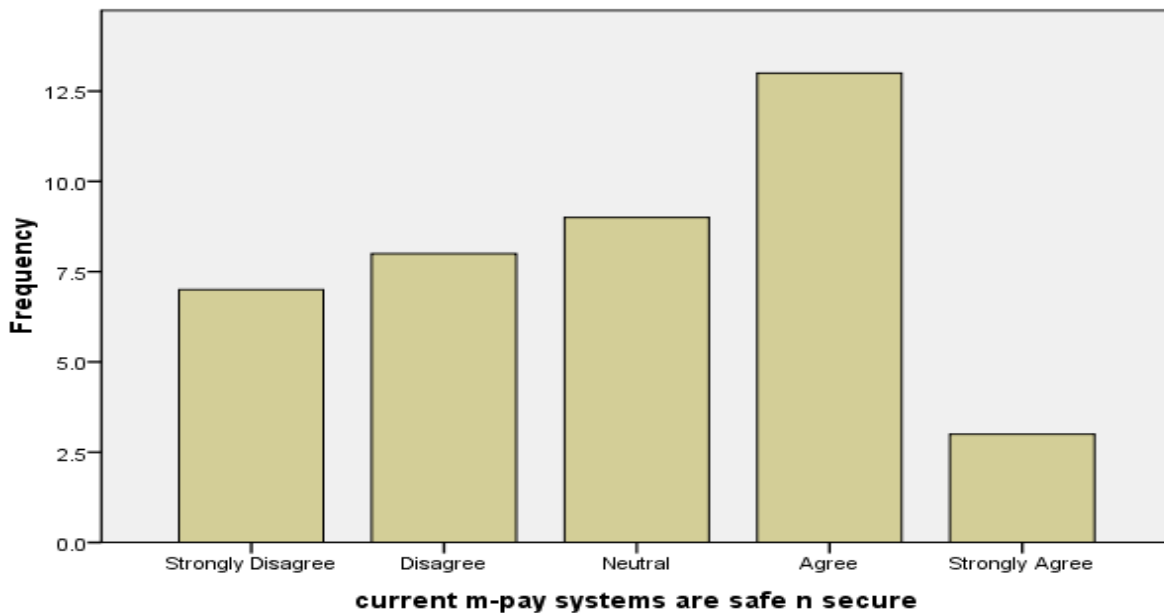


Figure 4.9: Respondents response on whether current m-pay systems are safe

4.10 Does Education Level Affect The Use Of Mobile Payment By

The Respondents

		Do Respondents Use Mobile Payment	
Education level of respondents		Yes	No
Primary	Frequency	4	5
	% of Total	10.0%	12.5%
Secondary	Frequency	14	4
	% of Total	35.0%	10.0%
college/university	Frequency	6	7
	% of Total	15.0%	17.5%
Total	Frequency	24	16
	% of Total	60.0%	40.0%

Table 4.10: Crosstab of education level against mobile payment use

Table 4.10 above shows the education level of the respondents and those who use mobile payment applications. From this table we see that most of the respondents who use mobile payment applications have secondary education followed by those who have had university education and lastly primary education. While similarly those who had university education opted not to use mobile payment applications in their businesses. This shows that a majority of the respondents who use mobile payment application are those who have secondary education and university respondents don't use mobile

payment applications in their businesses. This is as shown in figure 4.11 on the next page.

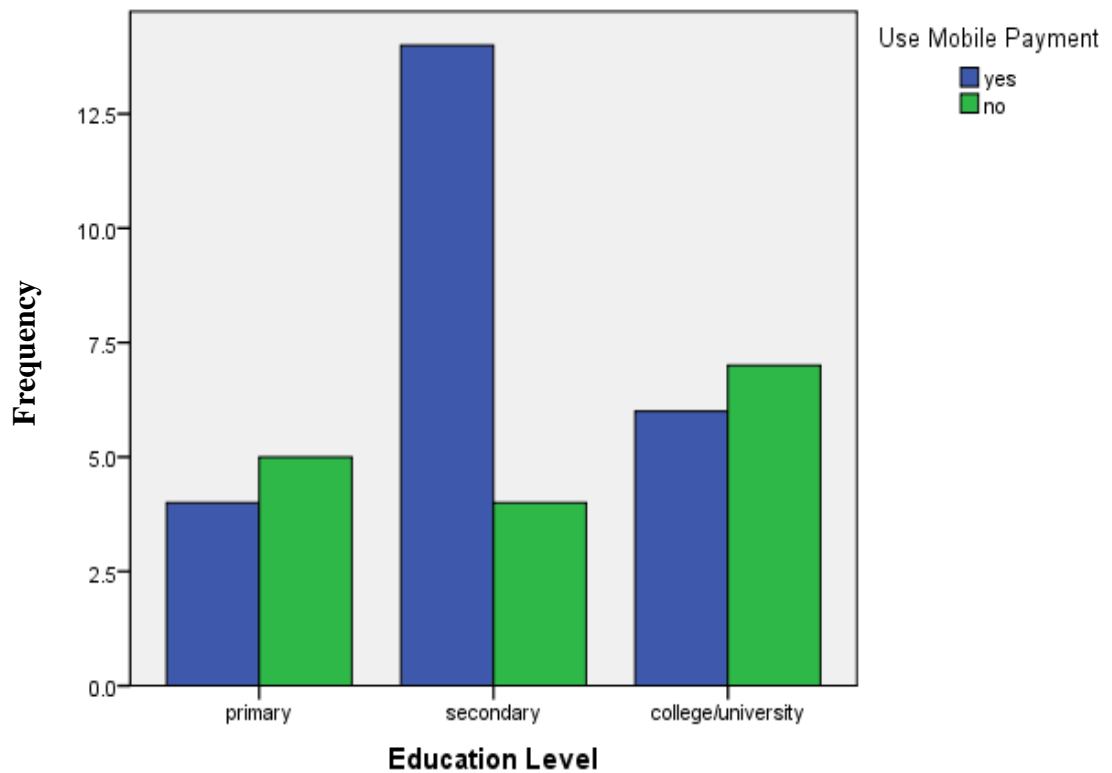


Figure 4.10: Education level against mobile payment use

From the above bar graph respondents who had education past primary school tended to use mobile payment application in their businesses. This is attributed to the fact that they had a high tendency for acceptance than their primary counter parts. On the same not, it is also noticed that only secondary school respondents agreed to use it more than their college/university respondents, this is attributed to the fact in figure 10 below where we see that a majority of the respondents who had secondary school education deemed that these applications are safe and secure as compared to their college respondents. Hence they would agree to use them in their businesses.

4.11 Education Level Affects The Attitude Of Respondents Towards

Mobile Payment Applications

Education Level	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
Primary	3	0	1	4	1	9
Secondary	1	4	5	7	1	18
College/University	3	4	3	2	1	13

Table 4.11: Education level and perception of mobile payment use

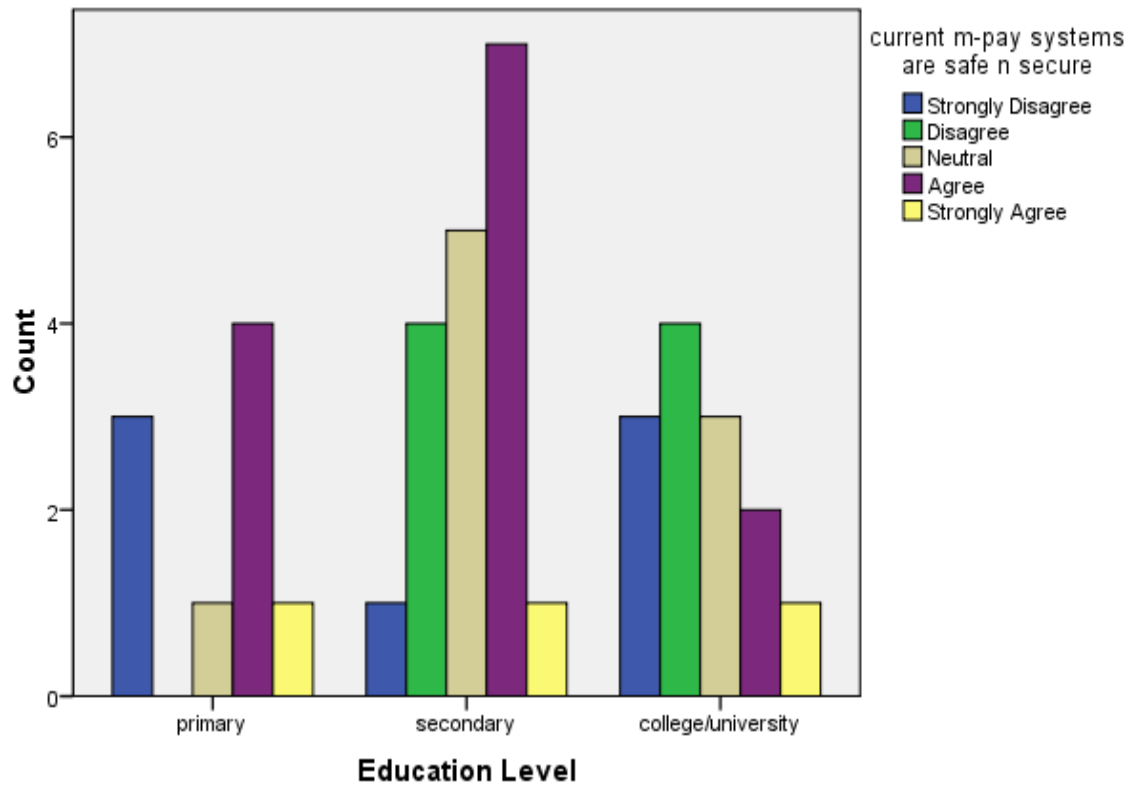


Figure 4.11: Education level against perception of mobile payment

The figure 4.11 on the previous page portrays the respondent's attitude towards the security level of these mobile payment applications in use today. It depicts clearly that respondents who had secondary school education deemed that these applications were highly safe and secure thus attributing to their huge score in the agree column, which is further shown in figure 4.11 that they were the ones who had the highest score when it comes to using mobile payment applications in their businesses. College/university respondents however showed in their response that they felt these applications were unsecure together with their primary counterparts who had the highest score for those who felt these applications were unsecure.

4.12 Do the Respondents Favor the Proposed Approach Of Enhancing Pin

Respondents favor proposed enhancement	Frequency	Percent
Disagree	6	15.0
Neutral	7	17.5
Agree	19	47.5
Strongly Agree	8	20.0
Total	40	100.0

Table 4.12: Those who favor for enhancement of PIN

Figure 4.12 on the next page shows how the respondent's thoughts on whether to enhance PIN with timestamps. The pie chart depicts that most of the respondents are in favor of this enhancement which is 47.5% combined with 20% for those who strongly

agree. This was due to the fact that as was shown in the challenges they faced, many were of the loss/theft of their PIN and also due to mobile fraud

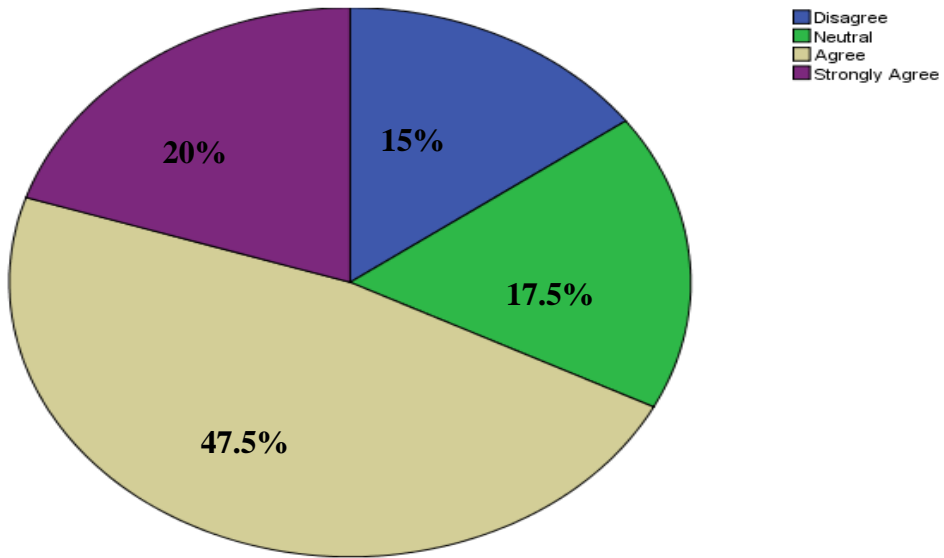


Figure 4.12: Response of those in favor of enhancing PIN

4.13 Respondents thought on the current safety of transactions

Respondents attitude on current safety of mobile transactions	Frequency	Percent
Disagree	6	15.0
Neutral	12	30.0
Agree	15	37.5
Strongly Agree	7	17.5
Total	40	100.0

Table 4.13: Response on safety of mobile payment application

Figure 4.13 on the next page shows how that most of the respondents agree that current mobile payment systems offer safe transactions or keep their transactions safe which were 37.5% and 17.5% for agree and strongly agree respectively. A number of them still viewed them as being unsafe due to the challenges they faced while using these applications which was around 15%.

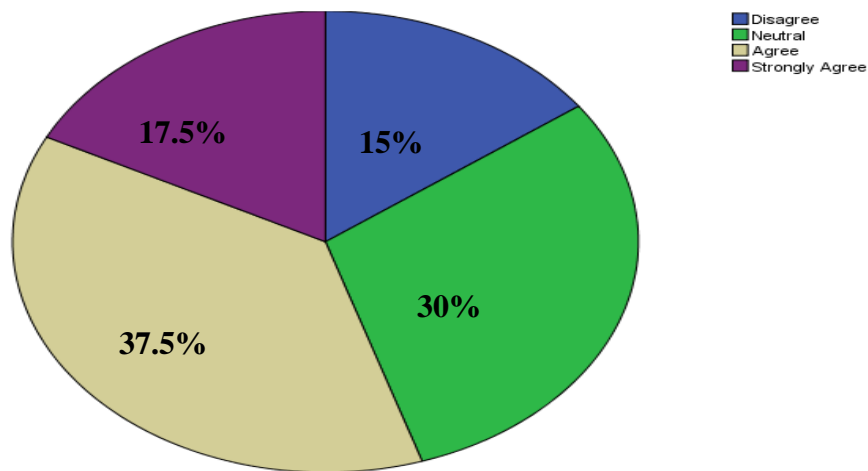


Figure 4.13: Response on safety of mobile payment applications

4.14 Respondents Thoughts On Current Non-Repudiation Mechanisms In Mobile Payment Applications

Respondents response on current non-repudiation mechanisms	Frequency	Percent
Strongly Disagree	5	12.5
Disagree	8	20.0
Neutral	13	32.5
Agree	14	35.0
Total	40	100.0

Table 4.14: Response concerning non-repudiation mechanisms

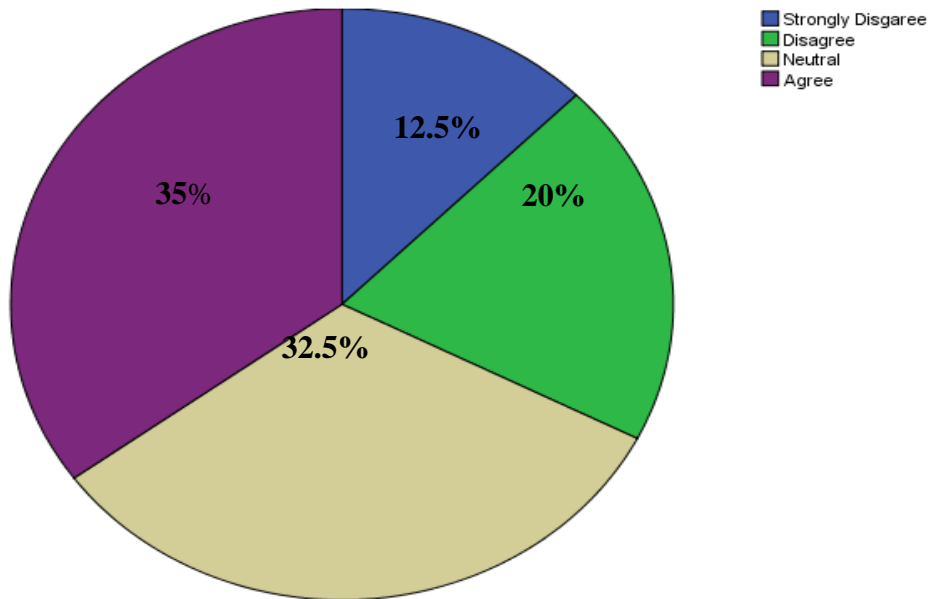


Figure 4.14: Response concerning non-repudiation mechanisms

Figure 4.14 above shows that a majority of the respondents didn't agree or strongly disagreed that these applications offer good non-repudiation mechanisms. Although in the chart it shows that 35% of the respondents agreed we see that about 65% of the respondents still either were neutral or they disagreed with this notion. This is attributed to the fact of the challenges they faced which included PIN theft and also mobile fraud.

4.15 Conclusion

From the analysis conducted, it was sufficiently able to answer the analysis objectives. From the presentations of the bar graphs and pie charts for the various objectives, one is able to draw clearly the domain within which the proposed approach will be implemented in.

Through the analysis one is able to know that most of the business people involved in the study in Thika town readily agree to use mobile payment applications to transact with their customers. This is easily supported with the communication commission of Kenya (CCK) quarterly report for the period of October-December 2011/2012 where they tell in full that the total numbers of subscribers to these services are 18.9million people and they are mostly people who don't have access to bank accounts that makes the bulk of this number.

The mechanisms that most respondents have knowledge in are also known through the results of the analysis. The authorization mechanism which is known by most respondents is the PIN mechanism. Also passwords and user accounts are known by the respondents because when one wants to open up a mobile payment account, they are usually provided with an account which is their mobile number and a secret word which is usually their password so that incase fraud occurs, it easy to ascertain that the line is actually theirs. For mobile payment challenges the respondents responded by giving their views on the challenges they faced. During the analysis it was noted that most of the respondents stated that sending of money to the wrong recipient was the major challenge, followed by theft of their personal identification numbers and cancellation of the wrong transaction. Also respondents spoke of mobile fraud which takes many forms one of which they stated as sending of fake transaction messages purporting to have sent money to their intended victims while in actually sense there wasn't any money sent. And as most of these victims of such schemes don't take to check their balance send money to the person and in due time realize they have been conned. The mobile service

providers also cited the issue of mobile fraudsters defrauding innocent customers of their money through fake transaction messages and also repudiating on some of these transactions. But the mobile service providers also stated what they do to try and curb these challenges.

Lastly the analysis gave a detailed view of the respondent's thoughts on whether the mobile payment systems being currently used are safe. The results showed that a huge number of them think that these applications are safe, but also a sizeable number seemed to lean more on that they were not safe. Hence the results of this analysis show that the respondents have a view that the current mobile applications are safe due to the measures taken by the service providers to ensure that they protect their customers.

The part of the mobile service providers on the responses to their questionnaire greatly helped in gathering the technical aspect of the proposed system. Through this it was easy to know how the current system was implemented and its technical details.

Below is a detailed description of how their mobile payment solution is in terms of technical terms.

They stated that they use the following to ensure that repudiation does not occur when people are transacting

- *Unique MSISDN and Password tied to the MSISDN. Presenting of ID or Passport on performing of M-PESA mobile transactions at agent terminals. Secret word for authentication of account. Unique transaction number for each transaction.*

The mobile service provider also stated they use the following authorization mechanisms

- *Valid PIN, secret word and Web portal interface credentials.*

The mobile service provider stated they have the following to enhance repudiation of their authorization mechanism which is the PIN. Though it is not in terms of what technical aspect they have added rather on the contingency measures they have undertaken to ensure repudiation is taken care of.

- *Customer awareness on enforcing PIN secrecy.*
- *Enforcing set up of PIN at Registration Process for M-PESA*

They also gave a description of they handle repudiation cases when they occur

- *Flag suspected transactions, Bar the Account and have this case transferred to the internal fraud section to follow through with the local authorities.*

The respondent also stated that they do store the information provided by the authorization and non-repudiation mechanism in their databases. This will mostly be used as evidence in case a problem occurs. The respondent also clarified that this information is stored in multiple repositories to enhance redundancy incase their might be a system breakdown which might result in loss of the very vital information. This information stored in the database shall be retrieved through use of queries and on-demand reports that shall be activated when one requires the information. The respondent also gave the procedures they undertake to ensure that no outside tampering of the database takes place and this is through having a strong security settings enforcement that is taken care of by the IT security team of the company. The

information stored in the database shall be used as evidence in case a repudiation case occurs. First the reports from the customers to the helpline and logs (include flagging limits and transaction trends) are searched for. Then a trend analysis of suspected accounts and transactions is done through use of the information/evidence provided usually the transaction ID.

The respondent also gave their views on which application platform that can be used to develop these applications and they stated that Linux, PERL, MySQL and VB.Net are the best platforms. For the main application VB.Net is recommended while for database application end he stated Structured Query Language or Oracle as the best tool to use to develop the database. It is not advisable to use java language which is usually in the programming suite J2ME. Debbai, Saleh, Talhi & Zhioua (2005) documents a vulnerability in some Java enabled phones that can be exploited to write a malicious MIDlet that sends SMS messages without requiring the user's authorization. This could affect the security of some SMS based schemes which require the user to send a SMS message (to the payment gateway) to initiate a transaction. If a malicious MIDlet is installed on the user's phone which sends SMS messages then it would be possible to initiate a transaction without the approval of the user. The best suited operating system was Linux as it is more stable than windows in terms of virus attack and connectivity on the internet.

For part of secure timestamps been implemented with PIN Mechanism, the respondent stated that already their transactions have already had atomicity enforced thus the timestamp feature being enforced on a real time basis. Thus the idea to tie it the Pin

would also enforce atomicity of the transaction even further. The use of Logs on the transactions ensures the durability of the transactions and reversals of the same too

Hence from the analysis, the key aspects found out were:

1. Most of the respondents had knowledge in Personal Identification Number mechanism as most of them had interacted with the current mobile payment applications in the market, hence their knowledge in it. Hence it would be easier to implement my proposed approach of using PIN.
2. The respondents also had knowledge in the use of timestamps in the current mobile payment applications. Thus the proposed approach sought to enhance PIN with secure timestamps.
3. From the mobile service providers point, the development suite they mostly preferred was VB.Net while for the database end they preferred oracle or structured query language (MySQL). The proposed approach sought to use C# which is a language used in VB 2008 and VB 2010 which has VB.Net in it. The reason for using VB.NET is because as stated earlier in the summary of findings, is that one vulnerability of Java enabled phones is that they can be exploited by fraudsters to write malicious MIDlet that send SMS without requiring the users authorization hence the need to choose VB.NET over J2ME because of that vulnerability. For the database end oracle and MySQL are the leaders in providing secure database applications which are secure and ensure data integrity.

4. For my proposed approach to work, the analysis from the mobile service provider involved in the study helped in understanding how they enforced non-repudiation and that was through the enforcing of atomicity of the transactions hence timestamp feature being implemented in a real time basis. Hence my proposed approach seeks to have an algorithm that would take the PIN, transaction ID and times the transactions were being done and have them as one non-repudiation entity.

CHAPTER FIVE

SYSTEM DESIGN

5.0 Introduction

This section entails how a system will meet the information requirements as determined by system analysis. The analysis part of the work helped in coming up with the system requirements for the proposed solution of enhancing PIN with timestamps to provide non-repudiation

5.1. How Analysis Informed My Design Criteria And The Algorithm

Analysis is greatly needed if one is to come up with a solution that caters for the problem domain and the people in that domain. Analysis helps the researcher to know the problem domain in depth, know what has been done to try and solve the problem. Analysis and literature review informed the design criteria greatly firstly through the choice of a development language because it helped in showing the limitation of java based mobile development languages like J2ME and the advantages of using VB.Net and C# in developing mobile payment applications. In the analysis findings it clearly came out that in order to provide an efficient non-repudiation approach in your application, it must have all the items involved in the transaction. Before, the proposed approach sought to implement PIN with secure timestamps alone, but after analysis it became clear that to achieve a higher level of non-repudiation other aspects like transaction ID, mobile number of both involved in the transaction have to be used in the proposed algorithm.

Analysis also helped in knowing that security has to be implemented from both ends, that is from the applications end and also the users end. Most applications in use are highly secure but the users fall to tricks used by these fraudsters like masquerading as mobile pesa agents and end up stealing money from them and also stealing PINs of the users. Hence users have to be reminded of how important it is to be on the lookout for these people or fraudsters.

5.2 Mobile Payment Architecture

The conceptual model/architecture for a mobile payment system usually involves 2 or more distinct characters based on the form of payment being done. As mentioned earlier in my literature review, mobile payment are of two distinct type the first being remote mobile payment applications and proximity mobile payment applications. The proposed application implements the two distinct types together. The conceptual model has the following actors

1. The consumer/ phone client who request for a service from a merchant and pays the merchant through the application. Should be a valid mobile payment subscriber and should own a mobile phone.
2. A merchant who provides goods or services to the consumer and accepts the payment from the user through a mobile payment application. Should be a valid mobile payment subscriber and should own a mobile phone.
3. Mobile service provider who provides the GSM network via which a transfer mechanism like use of Short Message Service or USSD can be used o effect

transfer and authorization of payments between the two. Also charged with billing the respective clients for either withdrawing or sending of the money to the respective person. Also ensures the authentication of the two parties involved in the transaction.

4. The PRSP and banks. Because the money in this payment scenario is virtual, there has to be a place where the actual hard cash is kept so that people can take it and also the accounts are virtual. For example there use of agents by the service providers to enable deposit and withdrawal of money.

5.2.1 Conceptual Model For The Mobile Payment System

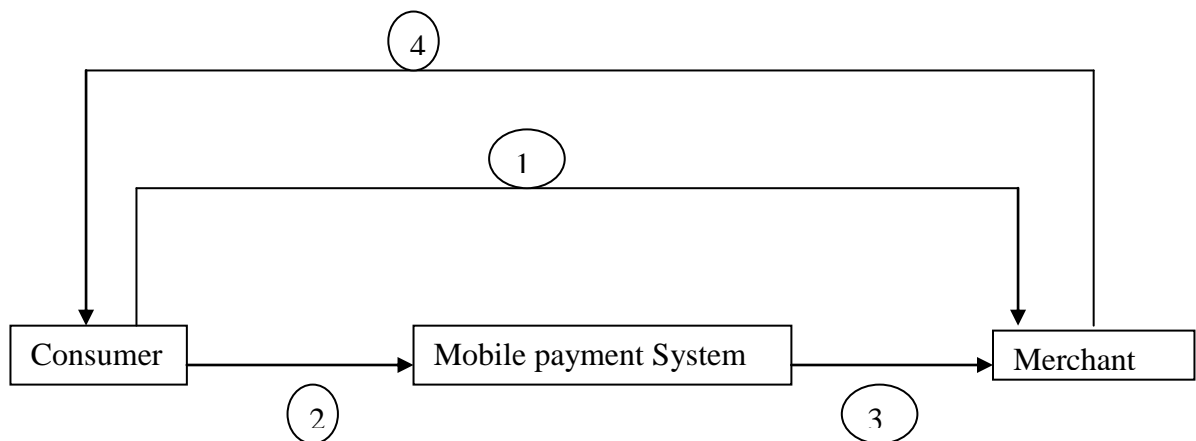


Figure 5.2.1: Mobile payment Conceptual model

The steps involved in this model are depicted using circles with numbers in them. The steps are:

1. The consumer selects a good or service they require for the merchant.

2. The consumer request for mobile payment service authorizes the transaction for fund transfer to the merchants mobile money account. The consumer receives the payment confirmation message detailing the name of the merchant, amount sent, time and receipt number
3. The merchant receives the payment information and confirmation message and name of the consumer who has did the transaction.
4. The merchant initiates the last part of any business which is the transfer of the goods or service to the consumer.

5.3 Architecture For The Proposed Mobile Payment System

The figure below depicts the architecture for the proposed mobile payment application. It is important to note that the billing of the consumer or merchant will entirely depend on the PRSP and mobile network operator involved and shall not be tackled in this model. The need for the billing is to show how in the end the proposed architecture shall be when it comes to implementation. The architecture comprises of both the consumer and merchant who shall have mobile payment accounts with the respective mobile network operator or any microfinance institution. The architecture depicts the steps involved when initiating and doing a mobile money transfer between two or more parties.

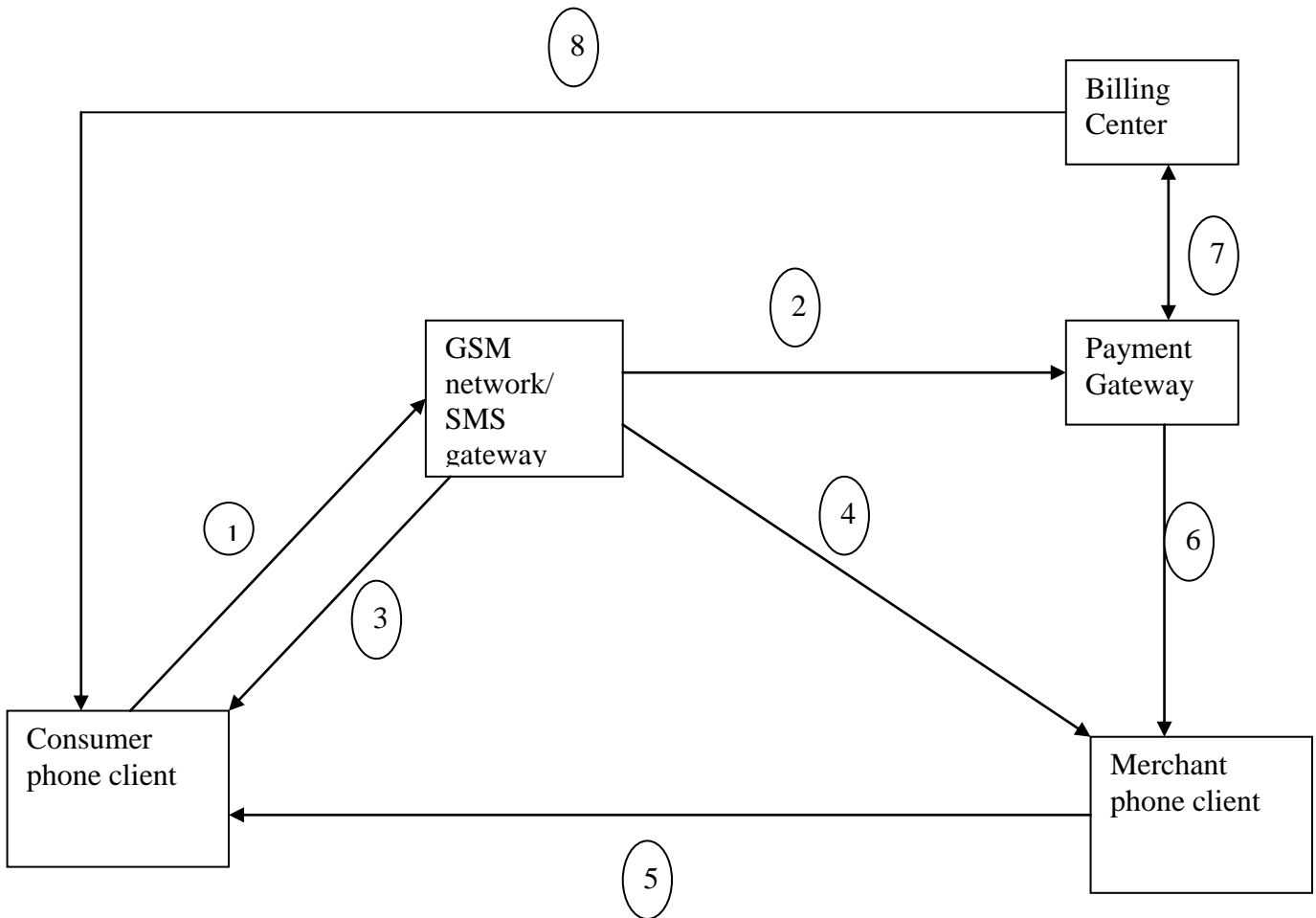


Figure 5.3.: mobile payment architecture

The steps for the model are depicted in circles with numbers in them. They are as follows;

1. The consumer phone client request for goods or services and then makes a payment request which is transferred to the GSM server. The request is in the form of an SMS.
2. The GSM server/mobile network operator transfers the payment request to the payment gateway and records the transaction.

3. The phone client receives a confirmation message showing that the transaction has been confirmed and payment has been effected to the merchant phone client's account.
4. The merchant phone client receives the confirmation of the payment transfer to his/her account through a confirmation message.
5. The merchant phone client delivers the product or service to the consumer phone client.
6. Merchant request for clearing through the payment gateway.
7. Payment gateway sends transaction records to the billing center.
8. The corresponding credited amount is recorded and included in the monthly bill and sent to the subscriber.

However steps 8 and 1 can be combined for the consumer phone client in that they can add the amount that shall be included in the bill for doing the transaction to the amount with which it is sent to the payment gateway and then to the billing center. This saves on time and cost for the mobile service provider.

5.4 Pin-Timestamp Algorithm

Because the main problem aspect of this project was to try and implement personal identification number mechanism with the timestamps mechanism in order to try and enhance PIN to provide non-repudiation. Thus in light with the problem statement, an algorithm was devised to try and see whether it would be possible to enhance PIN to provide non-repudiation through use of Time stamps. It is as follows

Algorithm: PIN, Time Stamp Algorithm

Algorithm PIN Time stamp Generation (PIN, Payer number, payee number, System Time)

Input Pin= P_1 , Stored pin = P_0 , TS=System Time, n =PIN Length, Input payer number = Pa_1 , Input payee number = Pd_1 , Stored payer number = Pa_0 , Stored Payee Number = Pd_0 ,
M= Mobile payment system, R= Payment request, ST= System Time, TS= Timestamp

NRO AND
NRR services
represented in
steps 1 to 7 of
the algorithm

Step1: Define SIZE: (size of the PIN length); $N = X$ where x is a certain digit

Step2: Find numbers of payer and payee. $M = Pa_1, Pd_1$

Step3: Check numbers if they are registered for the service in the database

Step 4: if (Payer number and Payee number= Stored Numbers):

They are registered for the service

Else Terminate request

$(Pa_1, Pd_1 = Pa_0, Pd_0)$

Step 5: Count Number of Characters of the PIN (Integer)

Step 6: Is it the correct PIN

Step 7: if (Count = Size) and PIN=Stored PIN

Correct Input and ready for authorization of transaction

Else return Wrong PIN;

$(P = N \mid P_1 = P_0)$

Step 8: Timestamp generated from the system time of the machine.

$ST = TS$

Step 9: Transaction Id, Date/Time, Payer and Payee numbers, amount and PIN are counter checked before request is committed and stored temporarily in the in_msg table.

Step 10: The Payer and Payee numbers, Transaction Id, amount and Date/Time of transaction being stored as in the out-msg table.

$M = (P_1, R(Pa_1, Pd_1), TS)$

Step 11: Send message with confirmation of the payment request

NRT service represented from step 8 to 11 of the algorithm

Using this algorithm the application is able to verify the correctness of the PIN, the time the transaction was effected together with the transaction ID and also the storage of the correct log which shall be used in case fraud or a case crops up. The above algorithm corresponds for Non-repudiation of Origin (NRO) , Non Repudiation of Transit and Non Repudiation of Receive (NRR) where the whole request is checked whether its' correct and timestamp added to it to indicate the time it was done. NRO and NRR are done in steps 1 to 7 in the algorithm. This is where the details of both parties are verified before the request is done. NRT is done in steps 8-11 of the algorithm where the timestamp

details are effected into the transaction request and are stored in the out_msg(out message table in the database).

5.5 System Design.

The main form of design modeling used was the unified modeling language (UML). This language consists of designing the system from the initial phase which is the use case diagrams up to the state diagrams.

5.5.1 Use Case Diagram

The figure 5.5.1 below is a use case diagram for the proposed system. The figure above was constructed through the use of the star UML software. The use case diagram usually helps in denoting what the various entities in the proposed will be, what their actions shall be, whom they shall interact with. The above diagram contains the main characteristics found in a class diagram namely

1. Actors: these are usually roles played by a user in the proposed system. in the above figure the actors are:
 - a. Customer(payee): this is the person who usually is concerned with making the payment
 - b. Business: actor entails the person receiving the payment from the customer
 - c. Mobile network operator: provides the GSM network infrastructure that shall be necessary in the transfer/sending of the payment messages from

the client to the mobile payment application and then in turn from the mobile payment application to the merchant's phone.

In the above use case diagram, both the client and the merchant have the same functionality in that they can both do payment request, withdraw, query account status from their handsets

2. Use cases: depict externally required functionality: the use cases involved here are the Payer login which shall be done when the user access their mobile phone, typing in the payment request and submitting the payment request, checking the PIN in the payment request and authorizing the request if the PIN is correct. Also the other use cases like receiving and facilitating the transfer of the request to the mobile payment application are also shown in the diagram

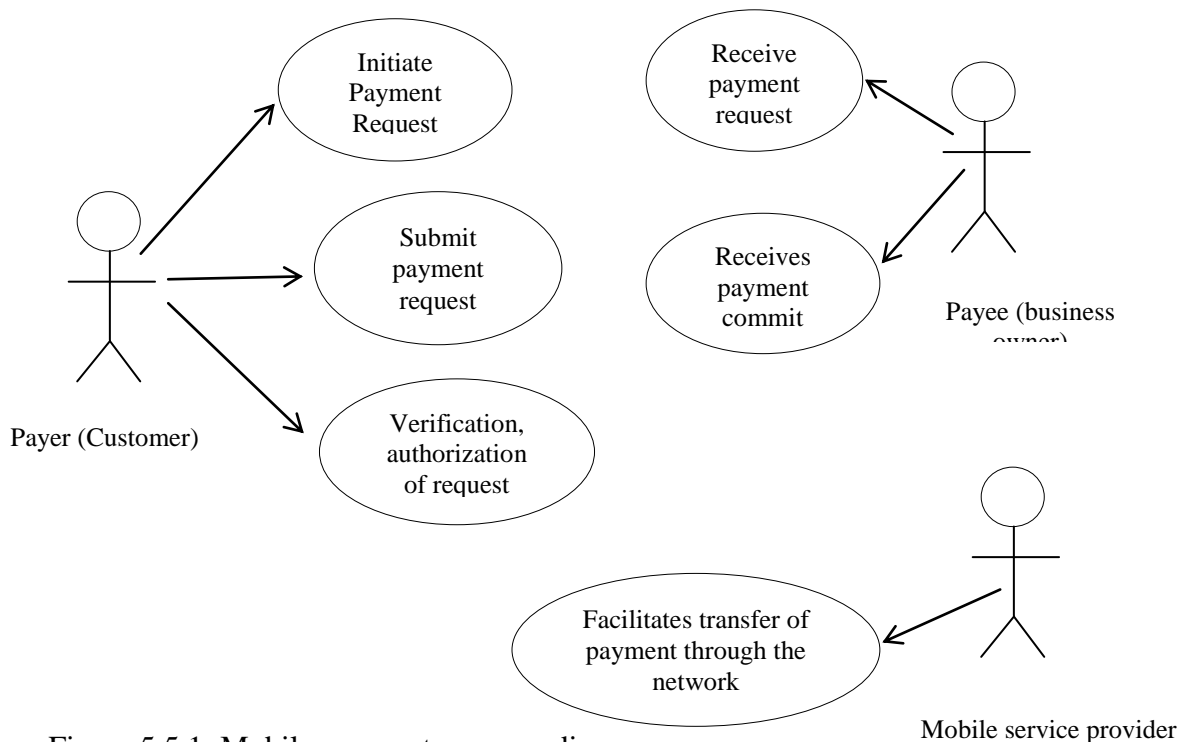


Figure 5.5.1: Mobile payment use case diagram

5.5.2 Sequence Diagram

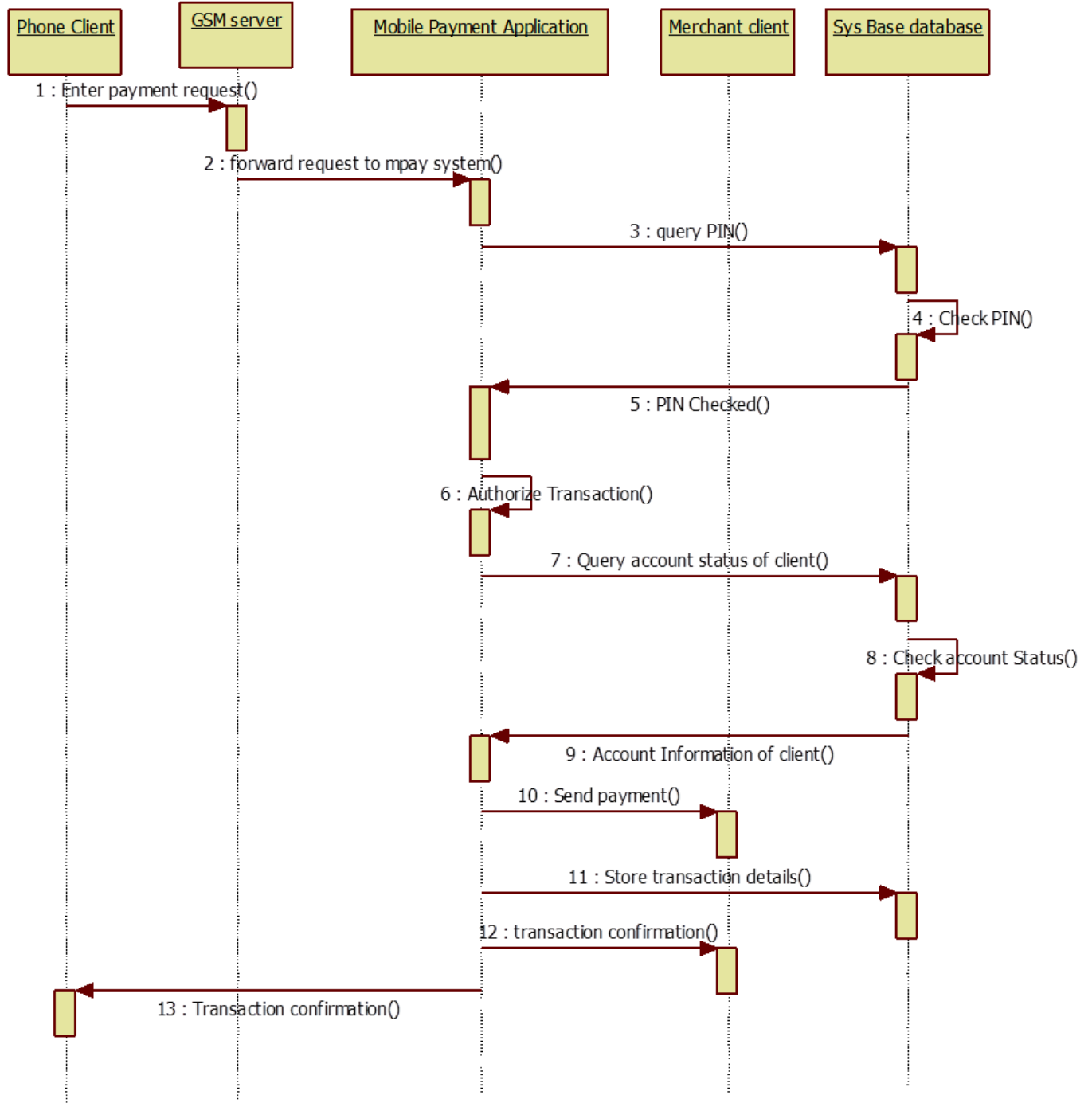


Figure 5.5.2: Mobile payment Sequence diagram

In figure 5.5.2, the diagram is known as the sequence diagram. This is graphical representation of system objects on time flows and the connections between the flows. The vertical dashed line is called the objects lifeline and it represents the objects life during the entire interaction. Each message is represented by an arrow between the life lines of two objects. The objects are shown as boxes at the top of the dashed vertical line. In figure 5.5.2 above we see clearly the objects that have been defined as the:

1. Client mobile: in this object the client uses a mobile phone to initiate a mobile money transfer between themselves and the merchant. The client writes an sms which is specified in a special format to differentiate it from other sms as a payment sms. He/she then sends the sms that shall be routed via the GSM network or the sms gateway application that shall be used to emulate the GSM network. The message or activity here is send sms with amount, merchant mobile number and PIN code to authorize transaction.
2. GSM/SMS gateway: this object represents the mobile network infrastructure that is responsible for sending and receiving of messages between the client and the merchant. It is responsible for channeling the message to the mobile payment system.
3. Mobile Payment application: It is responsible for accepting the payment request, validating the PIN entered and authorizing the transaction if the PIN entered is the correct PIN. It is also responsible for displaying authorization and confirmation of transaction messages to both the client and the merchant if all

goes well with the transaction. It is also responsible for crediting and debiting the accounts of the merchant and the client respectively.

4. Merchant: this object represents a person who is involved in the transaction with the client. The merchant receives the confirmation message stating that funds in their accounts have been credited after the transaction. This message acts as proof of receipt by the merchant of the funds. For the merchant to withdraw this money he shall have to go to an agent of the mobile service provider or financial institution that implements this application so that he can be able to withdraw and get hard currency.
5. Sys Base: it is the database that shall be used to store the applications information. The database shall hold the PIN of the clients, their account balances and status of the transactions that are being done. The database shall act as the repository for the transactions being done by the applications.

The client also receives a similar message stating that funds have been transferred from their account to the merchant's account thus acting as evidence that the transaction was done and that the correct person received the money.

In this proposed application it is important to state that all these transactions are virtual in that a person has to access a withdrawing point either from the financial institution side or the mobile service providers in order to get hard currency.

5.5.3 Mobile Payment Request State Diagram

In figure 5.5.3 below, the diagram is known as the state diagram. This diagram helps in describing the behaviour of the system. It will help in showing all the possible states a particular object can get into and how the object's state will change as a result of events that reach the object. Hence figure 5.5.3 shows clearly how a user makes a payment transfer to another user through use of the proposed mobile payment application. As shown the first state is whereby the user makes a payment request by inputting his PIN code, amount, number of the merchant and sends the SMS. The request is received by the SMS server which forwards it to the mobile Payment application for processing. Here the application checks both numbers involved in the transaction (both for the client and the merchant), the account balances of the two, checks the PIN inputted by the client to authorize the payment. If the PIN inputted is correct, the transaction is authorized and the transfer of funds is effected. The application ensures that the transaction is correct and then completes the transaction. The details that is the confirmation messages are sent to both sets involved in the transaction. The transaction logs are stored in the database. The logs stored in the database contain the transaction id, time the transaction was done, the PIN, senders and receivers numbers and the amount of the transaction.

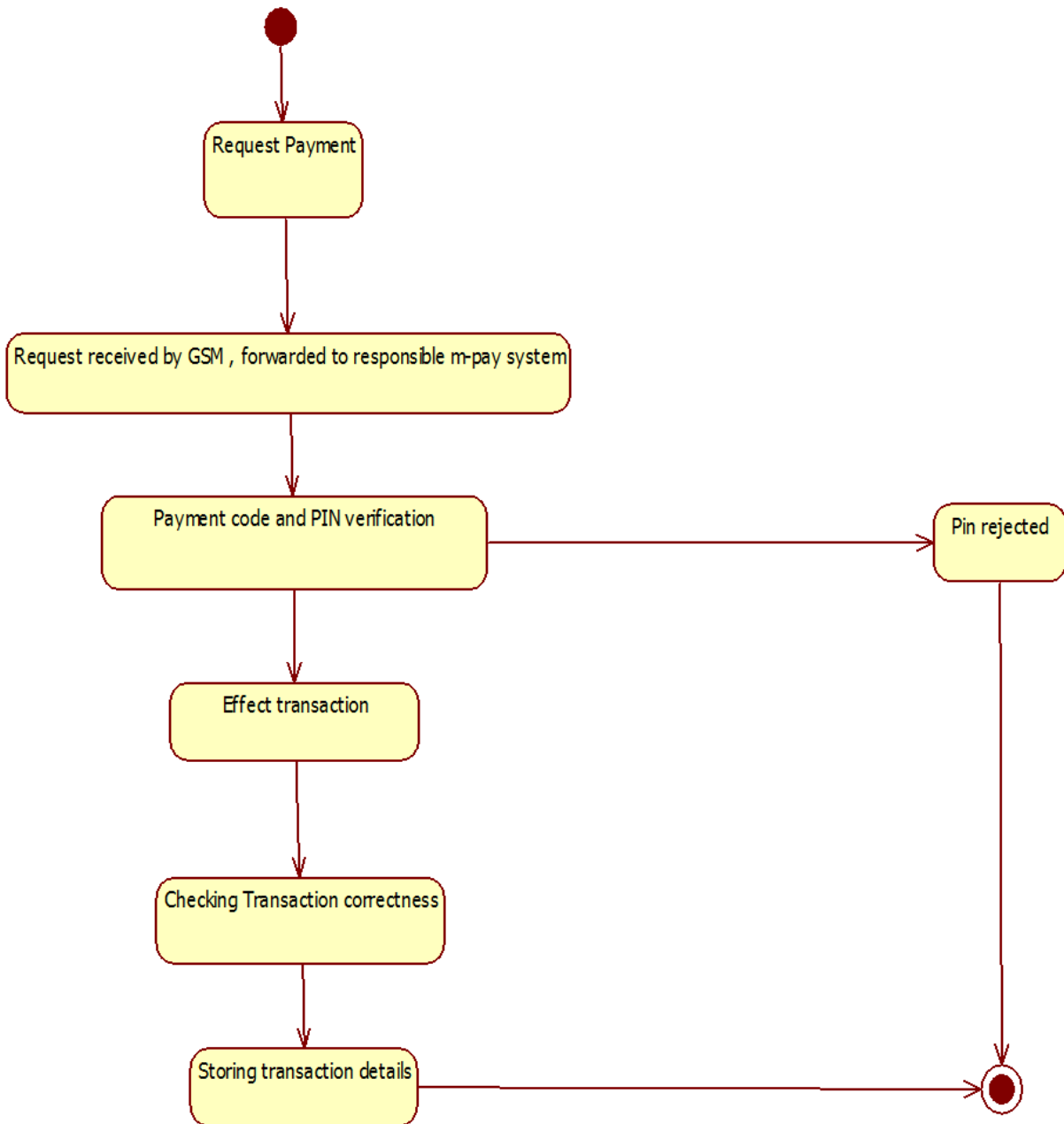


Figure 5.5.3: Mobile payment request State diagram

5.5.4 Mobile Payment Class Diagram

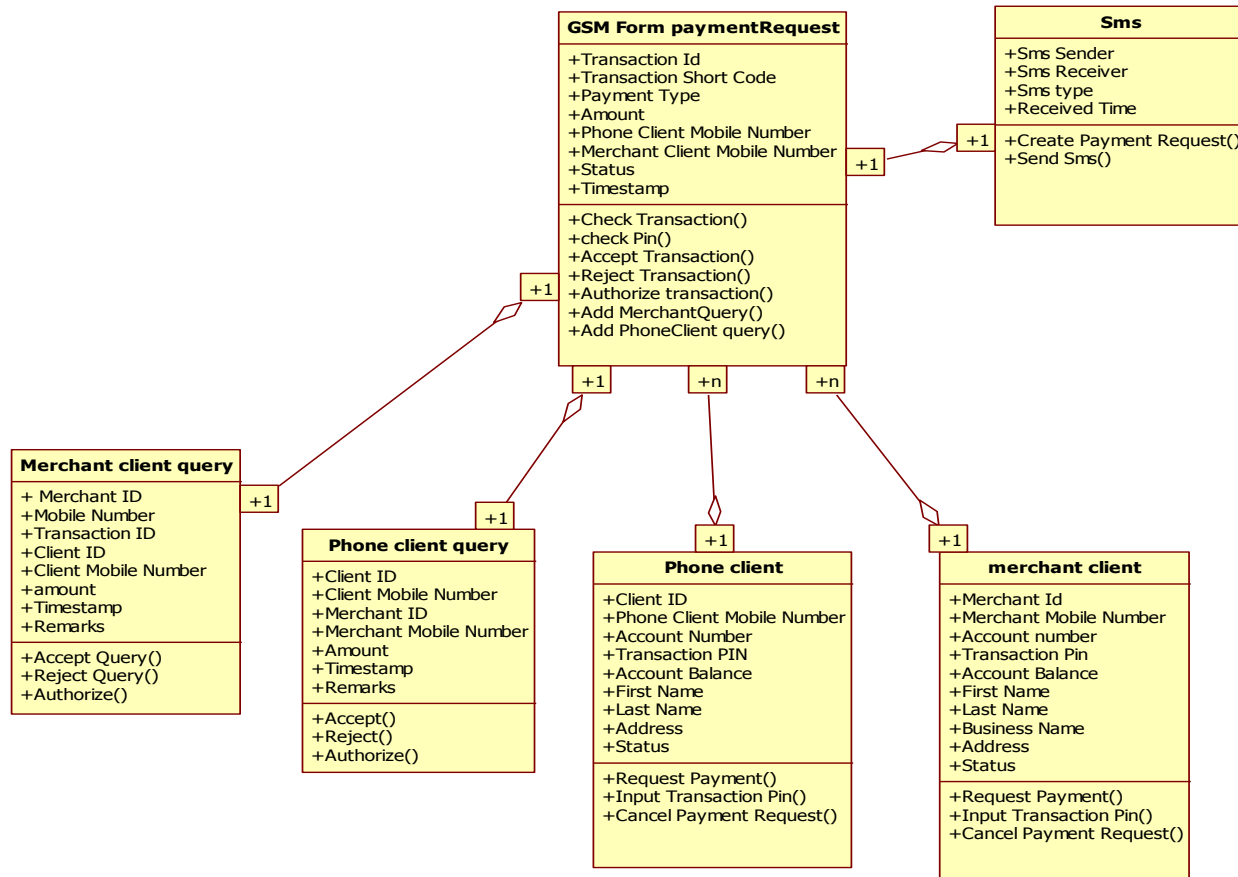


Figure 5.5.4: Mobile payment Class diagram

Figure 5.5.4 above shows the class diagram for the proposed mobile payment application. The class diagram contains the major class which is the GSM Form Payment request; this class is the major class that shall be used in doing the payment request for the client and merchants. The merchant query and client query classes are used by the GSM form payment request to query the account status of the merchant and client, this is necessary because a transaction will not be done if the account is below the transfer amount. The phone client and merchant client classes contain the details of both

the merchants and the clients. Here when authorizing a transaction the GSM form payment request shall check the PIN in these classes in order to ensure that only the correct PIN is used to authorize the transaction.

5.5.5 Mobile Payment Request Activity Diagram

An activity diagram shows task that need to be done by the application and the users of that system, in this case the phone client to initiate a payment request. Each activity follows the other in a sequence that is orderly. They help in elaborating work flows within the system. The tasks are clearly outlined in the diagram. The diagram starts from the point where the phone client keys in a specific code requesting to do payment. The code is the form of Amount # Merchant Number # PIN which the client sends to the number that shall be used by the mobile payment application. This is sent in the form of SMS to the SMS server. The SMS server checks the format of the SMS to check whether it's a payment request or a normal SMS through the destination number the user inputs and forwards it to the mobile payment system. The mobile payment system receives the payment request and checks the details of the SMS. First it checks the PIN the sender typed, if it is the correct PIN it enters the next stage of checking the balance of the sender. If the sender has enough money in the account, the application will go to the next stage whereby it verifies the number of the client where it checks the receiver's number. Then the application authorizes the transfer of funds from the sender to the receiver. There is a minimum number of 3 tries for the user in case they input the wrong PIN. If by three attempts the user has not keyed in the correct PIN the application will

terminate the payment request and send a message to the user stating that the PIN keyed in was invalid and the payment request terminated. Figure 5.5.5 below is the activity diagram for the proposed application.

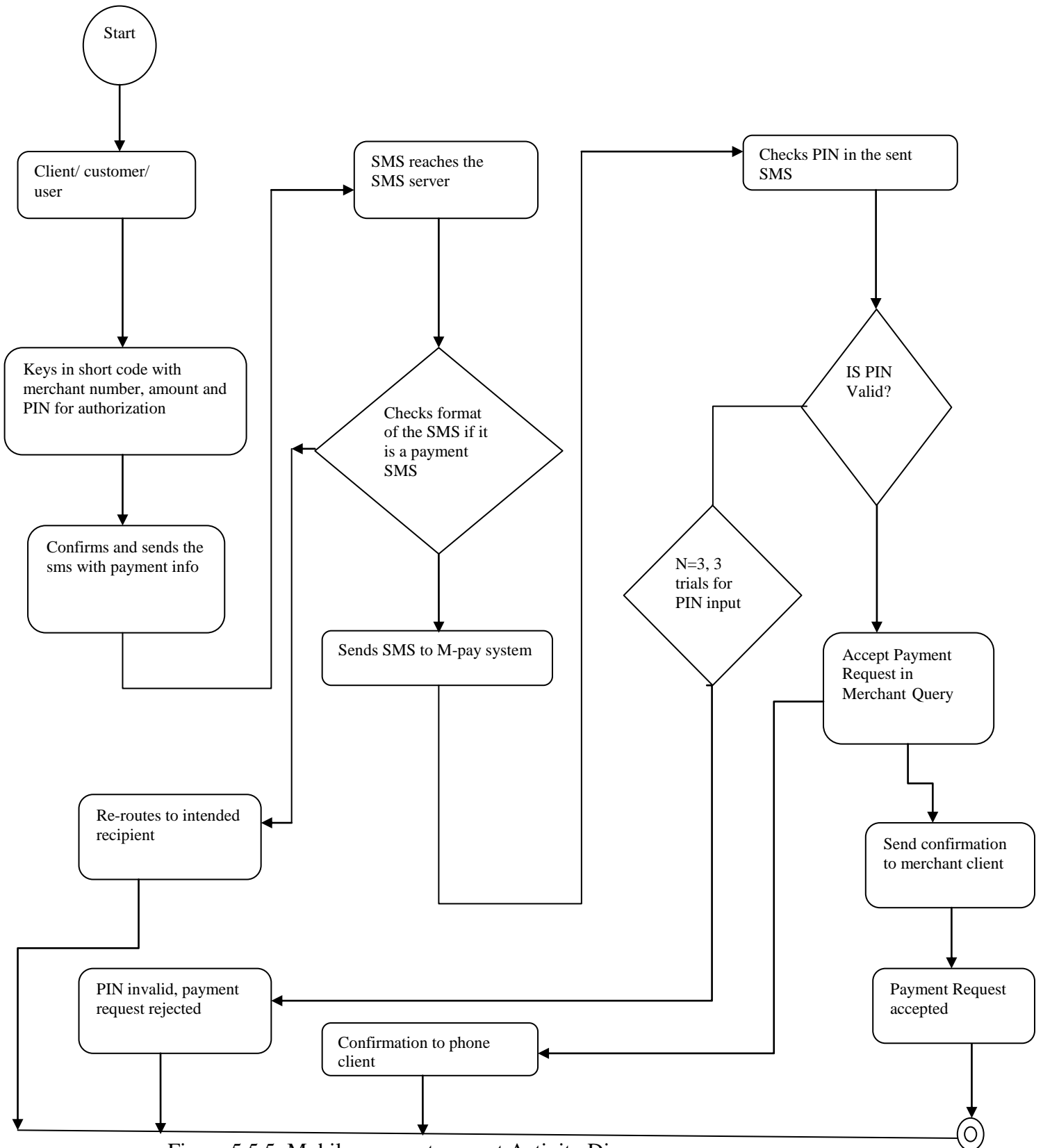


Figure 5.5.5: Mobile payment request Activity Diagram

CHAPTER SIX

EXPERIMENT AND RESULTS

6.0 Introduction

This chapter explains how the proposed solution was tested to verify whether it attained the main goal of the research, which was to enhance PIN to provide non-repudiation through use of timestamps. This chapter explains the requirements to conduct the experiment and also the results of the experiment

6.1 Goal Of Conducting The Experiment

The Main goal of doing the experiment was to ascertain whether implementing personal identification number (PIN) with timestamps would enhance the capability of the PIN mechanism to provide non-repudiation services. This would greatly aid in the reduction of mobile fraud being committed through these mobile payment applications.

Also through this experimentation, other aspects of the developed system will be evaluated like functionality of the proposed system.

The intended measure of this experiment was to check whether the system was able to have timestamps implemented with PIN mechanism.

6.1.1 Equipment Used In The Experiment

- For this experiment to succeed properly, it was deemed necessary to experiment the proposed system using a real mobile device instead of using emulators or mobile test tools. The reason for this is that emulators lack the real limitations being provided

for by the use of real mobile devices. That is the limitation exposed by the use of real devices is lacking in emulators, thus the test done on an emulator may function but when you transfer it to a real device and the limitations come into play the approach may not work at all. Also real devices depict the way users will input the payment request through use of their short message services, hence will be effective in pin pointing out mistakes carried out by people who are doing the payment request.

- A modem will also be needed as this will help in relaying the payment request to the application for processing.
- A SIM card that shall be used with the modem which shall aid in relaying the payment request to the mobile payment application.
- A laptop to run the proposed application. The laptop shall also have the SMS gateway that shall help in relaying the payment request to the application for processing and also do the confirmation messages to both sets involved in the transaction.

6.1.2 Setup And Conducting The Experiment

In this section I will detail the necessary setup for the project as well as the necessary administration requirements for the application.

1. First their need for a computer with minimum specs of processor speed 1ghz, 250Gb Hard drive, windows XP,
2. Development language used for the proposed application was the C# language which is found in VB2008 or VB2010 or VB.Net programming language suite.

3. SMS routing software like SMS server. This SMS gateway enables you to send and receive SMS's through your computer by use of your modem.
4. For purpose of the experiment it is necessary to have a modem, this device shall have a line which the users shall send the payment request to from which it shall be transferred to the payment application which shall process the transaction.
5. Sybase database to keep the information pertaining to the transactions.

There is need to have an SMS gateway that shall enable the transfer of SMS between two different mobile lines that shall be used in the transfer of payment. The free ware gateway that shall be used is the SMS gateway. This SMS gateway will help in queuing up payment requests and then transferring them to the payment application. The SMS gateway helps in sending and receiving of messages between your computer and a mobile device. The setup shall include the mobile device needed to initiate the payment request, the SMS server that shall forward the payment request, the proposed application that shall process the request, and the database that shall store the transaction details done.

The payment application will then process the request and forward it to the intended receiver. The application will then send a confirmation message to the users that the transfer has been done and store the details of the transaction in the database. The application will ensure that the accounts of those involved in the transaction are credited and debited respectively. The major aspect of this application will be in the authorizing of transactions, whereby it will check the provided PIN in the payment request against

the PIN stored in the database. If it matches, it will authorize the transaction else it will not authorize transaction in case of a wrong PIN given.

6.2 Experimentation Of The Proposed Application

The proposed application was successfully setup and run to see whether it would achieve the main objective and that was to enhance PIN with timestamps to ensure non-repudiation capabilities of the Personal Identification Number mechanism that shall be used to authorize transactions in the proposed approach. In the proposed application there are four components involved.

The users had to send a pre-formatted SMS that shall aid the mobile payment application to process the request. The format of the SMS is like <B, W, T, D> # <Number>#<Amount>#<PIN>

Where:

- Codes for <B, W, T, D>
 - B: Code for checking the balance
 - W: Code for withdrawing money from the account
 - T: Code for transferring money to the intended recipient.
 - D: Code for depositing money into the clients account
- Mobile number: Number of the intended recipient whom the transfer is being transacted to their account.
- Amount: amount that is being transacted
- PIN: PIN number that shall be used to authorize the transaction.

Break down of the elements used in the proposed mobile payment application.

1. Phone Client and Merchant client: represent mobile devices that emulate the basic functionalities of a mobile client and a merchant client acting as a wireless payment device. The client will need to authorize the transaction before the request is accepted by the mobile payment application while the merchant client will receive confirmation of the payment request from the client through the mobile payment application. Both will receive confirmation messages when the transaction has been completed detailing the time it was done, amount transferred, account balances and name of the person involved in the transaction.

2. SMS Server emulates the background functionalities of the GSM server employed by mobile network operators. The server basically receives the payment request from the client or merchant and forwards the message to the application for processing. Thereby after processing, it will again ensure that the confirmation messages are relayed to the prospective parties. The SMS server utilizes the modem and the SIM card inside the modem, from which respective forwarding of the messages will be carried out through the SIM card in the modem. In this case a SIM card belonging to the YU mobile operator was used.

3. The proposed mobile payment application will receive the payment request forwarded by the SMS server, check the PIN and authorize the transaction if the PIN is correct. The application will also ensure that the transaction details are stored in the secure repository or database.

4. Database that shall store the transactions being done. It shall also store the PIN numbers of the clients, hence when authorizing the transactions; the application will check the PIN number that was entered by the user against the one that was stored in the database.

Basically the phone client and merchant phone client emulate the basic functionalities of the mobile device being used as an electronic payment tool. The account of the phone client will be credited of the amount while that of the merchant will be debited of the same amount that the phone client requested to make a transaction of. The results of the transaction will be stored in the database.

6.2.1 Functionality Test

The purpose of the functional testing of the system was to gain certainty of the correct operation of the system. Thus the tests carried out focused on testing the system from the usage point of view. For this purpose the twenty people involved in the experiment were required to send and receive payment requests from which the following aspects of the functionality were tested:

6.2.1.1 CREATE A PAYMENT REQUEST

The phone client should be able to make a payment submit request with all the necessary details present. The details include the amount, number of the merchant and PIN to authorize the transaction

Test	Result
1. Submit a properly formatted payment request	The Payment request is accepted and processed by the application
2. Submit request with a mobile number that does not exist in the database	The payment request is rejected and system reports that one is not signed up for this service
3. Submit request with some important data missing	The payment request is rejected
4. Submit request with the amount specified in the request being more than the actual amount in the database	The payment request is rejected and system reports that one is trying to carry out a transaction that does not reflect the balance in the account.

Table 6.2.1.1: Results for the payment request functionality

6.2.1.2 AUTHORIZE PAYMENT REQUEST

The phone client after making the payment request and submitting it, the system should be able to verify whether the phone client and merchant details are stored in the database, which is if they are registered for the service. The application should also verify the PIN entered for authorization against the one stored in the database.

Test	Result
1. Submit proper PIN number in the payment request	The transaction is accepted and authorized. Payment is committed to the respective payee
2. Submit a PIN number in the payment request that is not stored in the database	The payment request is rejected and the system reports that the issued PIN is invalid
3. Number of digits in the PIN number does not correspond with the standard required for PIN numbers. That is either too many digits or less digits in the PIN number	The payment request is rejected and the system reports an invalid PIN issued by the client.

Table 6.2.1.2: Results for authorization of the request

6.2.1.3 COMMIT PAYMENT

The application should be able to commit payment to the respective number issued in the payment request and give a confirmation message to both parties that the transaction has being completed.

The two aspects are the core functions being done by the mobile payment application.

Test	Result
1. Commit payment with all the details correct and has being authorized	The transaction is authorized, done and confirmation messages sent to both parties of payment completion.
2. Commit payment with some details incorrect and has not being authorized	The transaction is rejected and the phone client is alerted over the error in the payment request.

Table 6.2.1.3: Results for committing the payment request

6.3 Security Test

The purpose of this test was to see whether non-repudiation could be provided for in the Personal Identification Number mechanism (PIN). From the proposed algorithm discussed in the system design, the aspect of implementing PIN with timestamps was tested in the application.

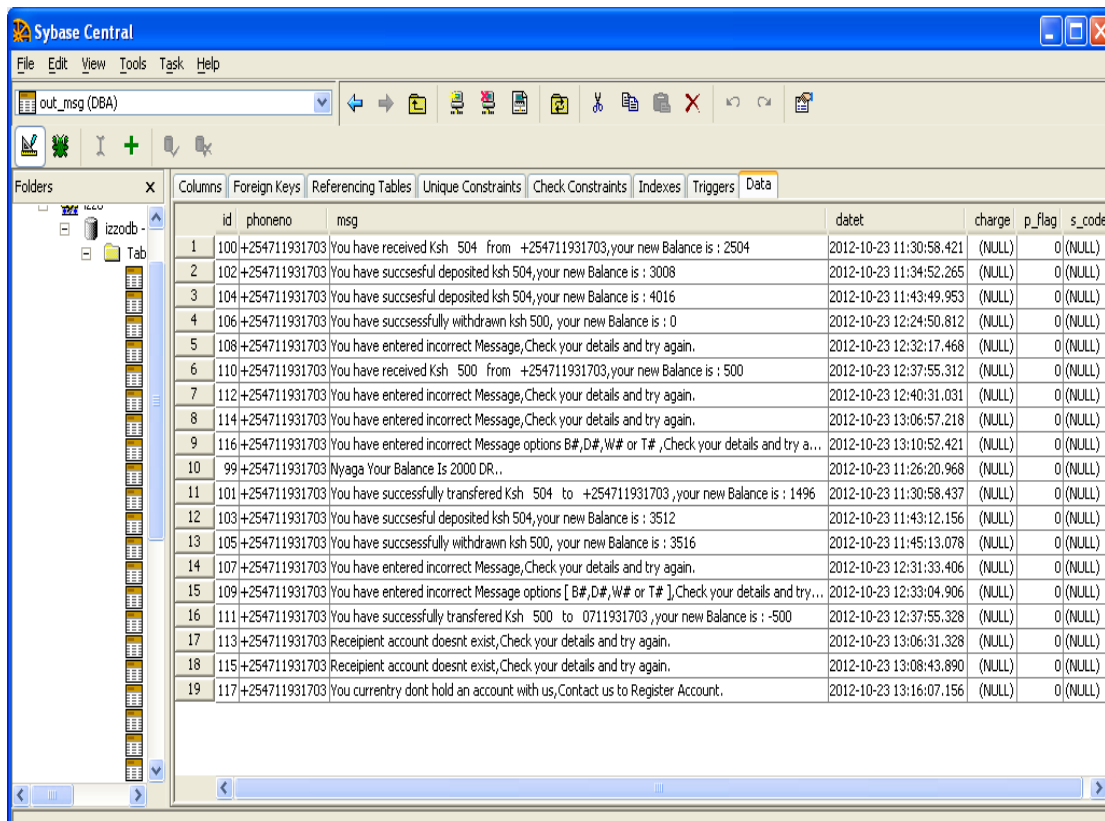
1. The first aspect of security was whether the system could authorize payments based on the PIN number being entered. It checked the PIN number provided for in the SMS with the one stored in the database for that client.
2. The pin which the user provided was checked against the one stored in the database.
3. During the checking of the Pin, another aspect was being formulated in the background because with every payment system the time aspect is every

important, thus the system was to record the time the request for payment was made. This time is based on the system time of the machine on which the application is running. The time is recorded in the database.

4. Thirdly was to check whether the applications repository offered a secure storage for the transaction details.
5. The capturing of both PIN, and the time at which the transaction was being done was also checked. This helped in checking the atomicity of the transactions based on real time of the system.
6. The application contains an out-message table which holds the messages that have been processed by the application.
7. The database also contains an in-message table which holds the incoming payment request. Immediately the request is received, it is forwarded for processing after which the message isn't stored because the application will keep on processing the request.

6.4 Screen Shots Of Some System Runs

6.4.1 Database Screenshot Of The Out-Message Table



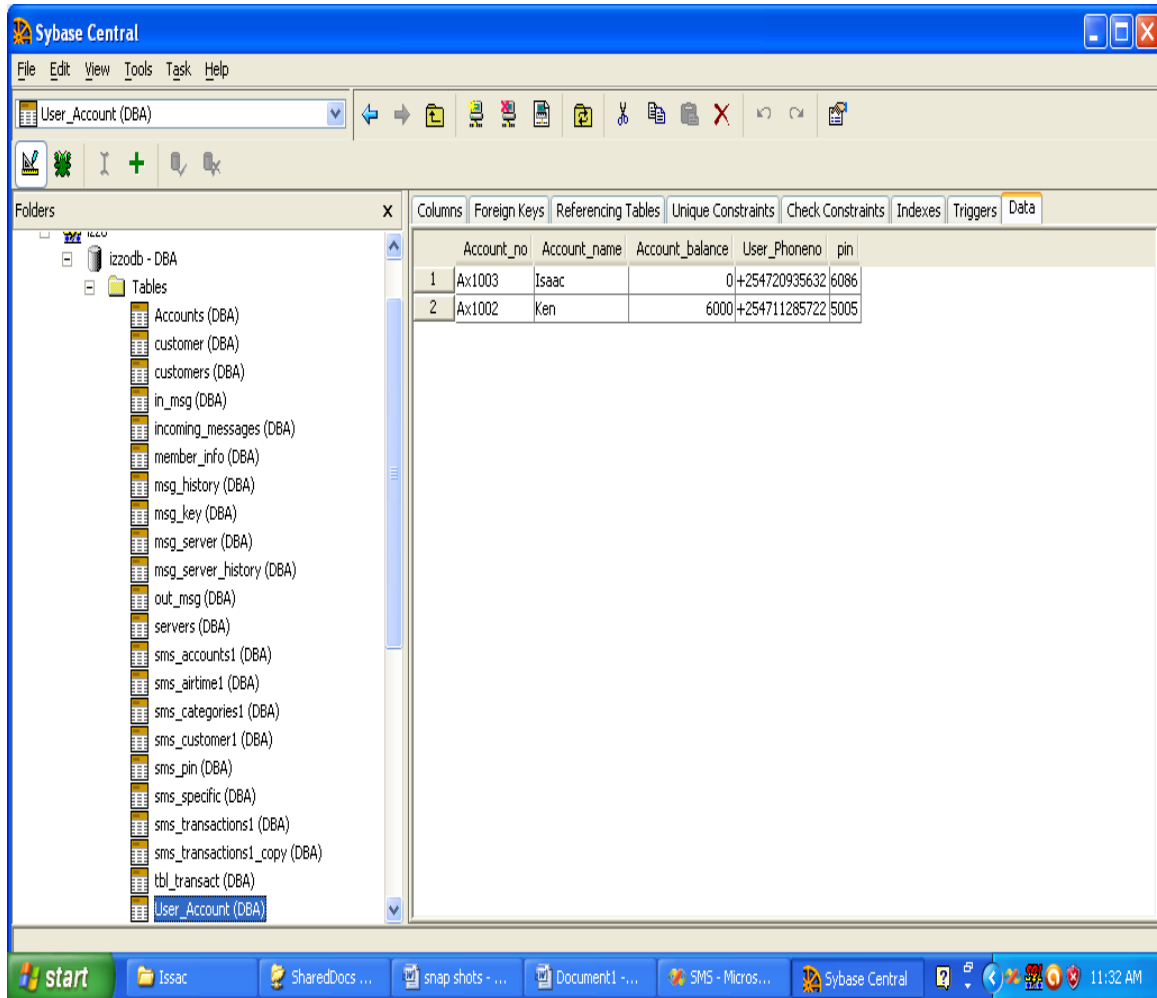
	id	phoneno	msg	datet	charge	p_flag	s_code
1	100	+254711931703	You have received Ksh 504 from +254711931703,your new Balance is : 2504	2012-10-23 11:30:58.421	(NULL)	0	(NULL)
2	102	+254711931703	You have succesful deposited ksh 504,your new Balance is : 3008	2012-10-23 11:34:52.265	(NULL)	0	(NULL)
3	104	+254711931703	You have succesful deposited ksh 504,your new Balance is : 4016	2012-10-23 11:43:49.953	(NULL)	0	(NULL)
4	106	+254711931703	You have successfully withdrawn ksh 500, your new Balance is : 0	2012-10-23 12:24:50.812	(NULL)	0	(NULL)
5	108	+254711931703	You have entered incorrect Message,Check your details and try again.	2012-10-23 12:32:17.468	(NULL)	0	(NULL)
6	110	+254711931703	You have received Ksh 500 from +254711931703,your new Balance is : 500	2012-10-23 12:37:55.312	(NULL)	0	(NULL)
7	112	+254711931703	You have entered incorrect Message,Check your details and try again.	2012-10-23 12:40:31.031	(NULL)	0	(NULL)
8	114	+254711931703	You have entered incorrect Message,Check your details and try again.	2012-10-23 13:06:57.218	(NULL)	0	(NULL)
9	116	+254711931703	You have entered incorrect Message options B#,D#,W# or T# ,Check your details and try a...	2012-10-23 13:10:52.421	(NULL)	0	(NULL)
10	99	+254711931703	Nyaga Your Balance Is 2000 DR...	2012-10-23 11:26:20.968	(NULL)	0	(NULL)
11	101	+254711931703	You have successfully transfered Ksh 504 to +254711931703 ,your new Balance is : 1496	2012-10-23 11:30:58.437	(NULL)	0	(NULL)
12	103	+254711931703	You have succesful deposited ksh 504,your new Balance is : 3512	2012-10-23 11:43:12.156	(NULL)	0	(NULL)
13	105	+254711931703	You have successfully withdrawn ksh 500, your new Balance is : 3516	2012-10-23 11:45:13.078	(NULL)	0	(NULL)
14	107	+254711931703	You have entered incorrect Message,Check your details and try again.	2012-10-23 12:31:33.406	(NULL)	0	(NULL)
15	109	+254711931703	You have entered incorrect Message options [B#,D#,W# or T#],Check your details and try...	2012-10-23 12:33:04.906	(NULL)	0	(NULL)
16	111	+254711931703	You have successfully transfered Ksh 500 to 0711931703 ,your new Balance is : -500	2012-10-23 12:37:55.328	(NULL)	0	(NULL)
17	113	+254711931703	Receipient account doesnt exist,Check your details and try again.	2012-10-23 13:06:31.328	(NULL)	0	(NULL)
18	115	+254711931703	Receipient account doesnt exist,Check your details and try again.	2012-10-23 13:08:43.890	(NULL)	0	(NULL)
19	117	+254711931703	You currentry dont hold an account with us,Contact us to Register Account.	2012-10-23 13:16:07.156	(NULL)	0	(NULL)

Figure 6.4.1: Out message table

This screen shot is for the out-message table. This table contains all the messages that after the request have been processed by the mobile payment application. As shown the table contains the time column, here the timestamp is implemented that shows the time the request was committed and the number to which the amount was transferred. Depending on whatever action the user choose, it will be captured in this database.

6.4.2 Database Screenshots Of The User Accounts

Figure 6.4.2: subscribed users account



The above database screen shot shows the database schema for the users who are registered for the mobile payment scheme. As shown in the shot, the table has the account number, account holders name, mobile number and PIN used in authorizing the payment. The application while authorizing the payment request checks the provided pin

with the stored in the database after which if it is the correct PIN, the application authorizes the request, if not it rejects the payment request.

6.4.3 System Interface Screen Shots

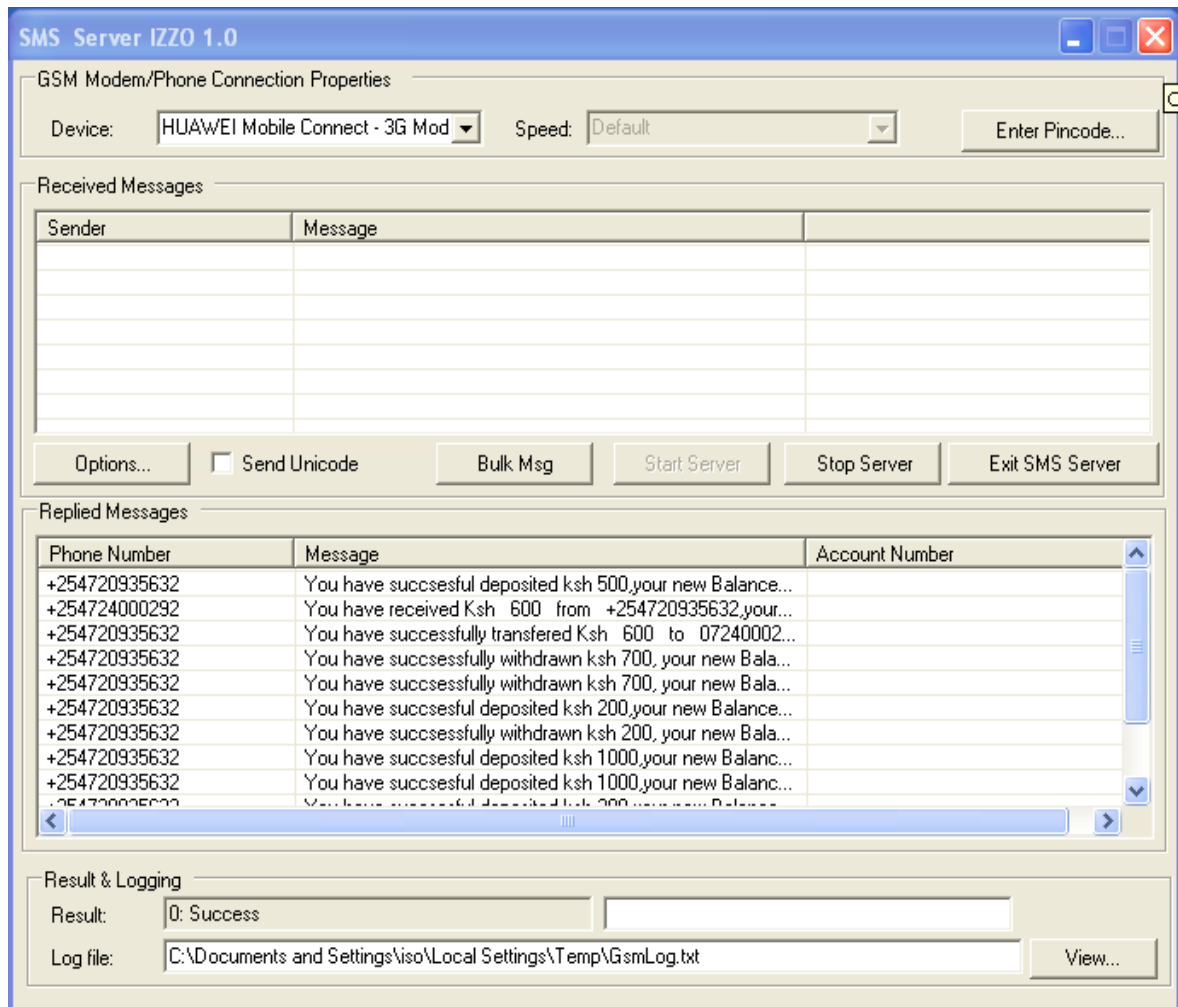


Figure 6.4.3: System interface screen shot

The above screenshot shows the system interface which is used in the proposed solution. The interface contains the replied and received sections which are linked to the database. These sections show the messages which the mobile payment application receives and processes the payment requests from the users. Only the replied messages can be viewed

as these are the messages indicating whether the request was successful or not. The replied messages cannot be viewed because immediately the request is received and forwarded to the application for processing it is deleted because the application will keep on looping on that message and process it several times leading to a failure in the logic of the application.

6.4.4 Screen Shot Of Mobile Payment Process

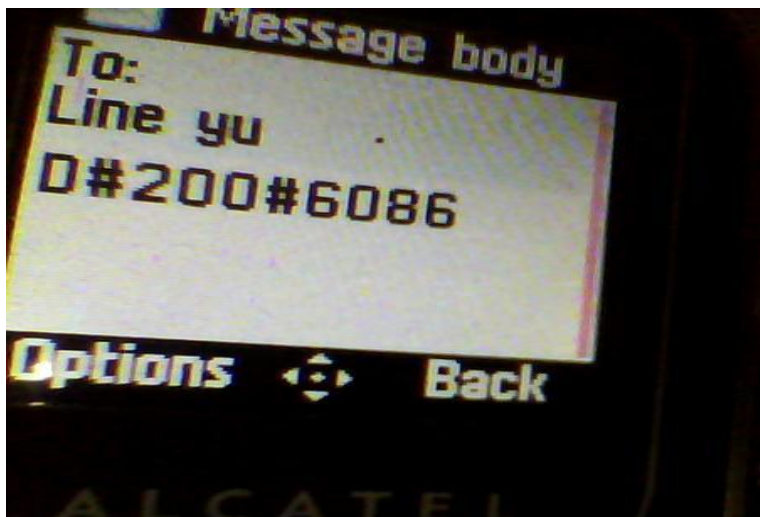


Figure 6.4.4.1: Screenshot for deposing money

The above picture shows a transaction request for depositing Kenya shillings 200 done to the proposed mobile payment application. D stands for deposit, 200 is the amount and 6086 is the PIN of the user doing the request.

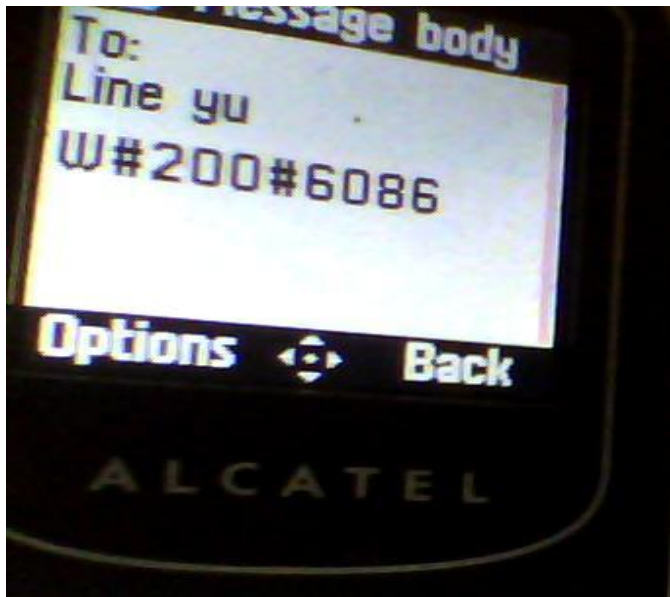


Figure 6.4.4.2: Screenshot for withdrawal

The picture above shows a payment request for withdrawing an amount of 200 shillings.

The message format is different for the above in that W stands for withdrawal. Each of the payment request detail is separated by the hash (#) tag.

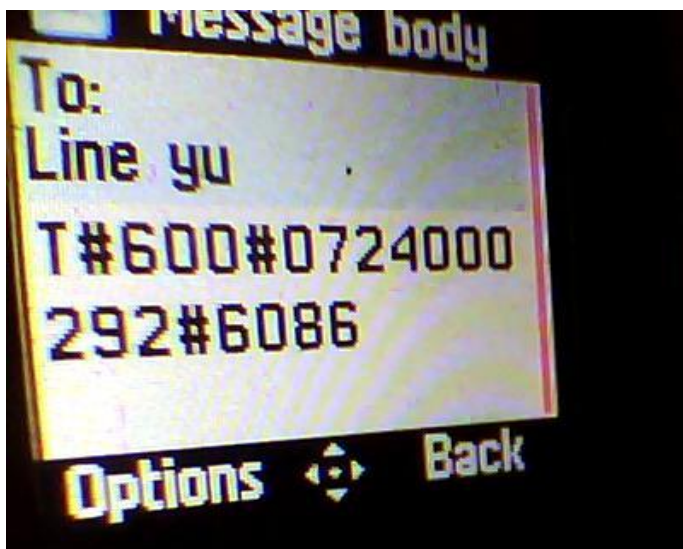
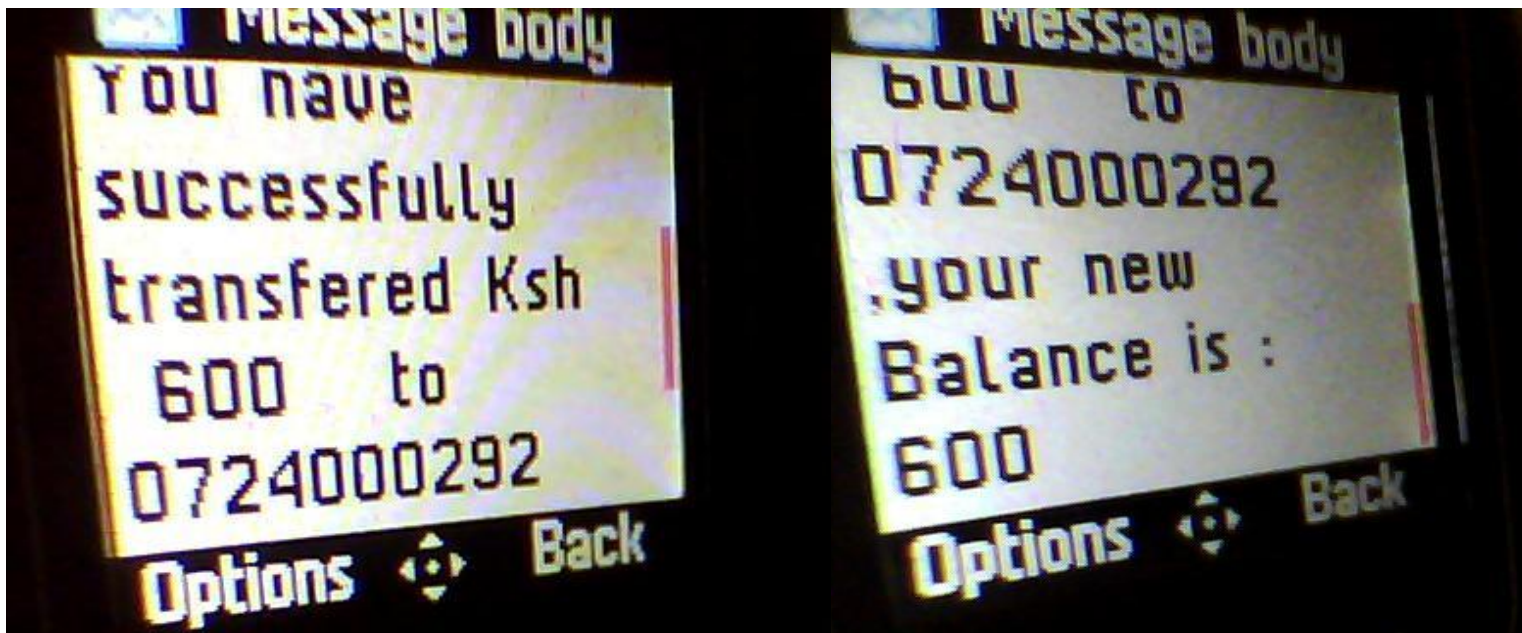


Figure 6.4.4.3: Screenshot for transferring money

The picture on the previous page shows a transaction request for transferring an amount of 600 to the number given. The transaction is identified by the unique code of T which



signifies to transfer funds from one registered user to another registered user.

Figure 6.4.4.4: Successful request Confirmation message

The figure 6.4.4.4 shows the confirmation messages after a transaction has been done, it gives the amount transferred, the number you have transferred to and the balance left in your account. Respectively the receiver of the transfer receives a similar message with the amount received, number received from and the new balance.

6.5 Results Of The Experiment

1. In the first aspect to be tested was whether the system could successfully authorize transactions based on the PIN number given by the phone client to do a payment request. The system was able to authorize transactions successfully

based on the PIN number given being checked with the one stored in the database for that particular client.

2. In the second aspect, the system time formulation was being checked. This is important because to effectively provide non-repudiation evidence, the time with which the transaction was done should be provided for in the application. The time was noted when the transaction details were authorized and stored in the database together with the transaction ID and mobile number used in the transaction. The three formed the highest basis of evidence generated by the application that a transaction was done.
3. The database offered secure storage services like encryption of the PIN stored in the database and only authorized personnel were able to access the application.
4. The aspect of atomicity was also checked for in the application. The application was to capture the time a transaction was effected, thus it was noted that the system was able to capture the time of the transaction being done effectively.

The overall objective of this project was to try and enhance PIN to provide non-repudiation through the use of timestamps. The objective was achieved because in the algorithm proposed in the design phase, sought to use both these mechanism which work independently of each other but the algorithm sought to have them work hand in hand to enhance non-repudiation in PIN The formulated algorithm was formulated to find a way to enhance PIN with timestamps. In most application these two are implemented separately but the algorithm sought to have them implemented together where after the mobile numbers of the parties had been verified the PIN was checked and thereafter a

timestamp generated that would indicate the time the request was sent. After the request was processed, the details pertaining to the transactions would be sent via sms to both parties and the details of those messages stored in the out_msg table and the accounts of those involved are debited and credited respectively.

The algorithm when implemented had to cater for other information that is necessary in applications that deal with money transfer such as the details of those involved in the transaction and the amount.

The algorithm further had to check whether those in the request were registered to use the service. If either of the parties was not registered the request would not be processed. For the request to be processed both parties had to be registered and the one doing the transfer had to enter the correct PIN to authorize the transaction.

During the literature review part of the project, it became evident of the measures taken by various developers to ensure that their products are safe and secure. Most evidently in the well-known M-Pesa mobile application much has been done to ensure repudiation does not occur like setting up of registration of users at M-pesa agents only. Even though the objective was not met it is evident in the current mobile-payment applications that non-repudiation of transactions has been achieved through enforcement of atomicity in the transactions, but what is necessary is the authorization of the transaction and the time it was authorized.. As it was discussed in the summary of the data analysis, one mobile operator sought to enhance user's awareness on the importance of ensuring PIN secrecy. This was through the various advertisements they have on both radio, television and on posters in the newspapers. Also the same mobile operator had set

strict mobile payment registration process where setup of PIN is done during the registration. The aspect of registration was not considered in this project as the issuance of PIN numbers to the registered users was not a part of this project. The project sought to work with already registered users who had already being issued with an account and thus had their PIN's issued to them.

Compared to what has been done in the banking sector with the use of ATM's (Automatic Teller Machines), whereby a random number is generated for a registered user who wishes to perform a transaction on the bank's ATM machine, this can be the next in line for mobile payment systems whereby for each transaction being done a unique number is generated by the application for the user to use.

CHAPTER SEVEN

EVALUATION, CONCLUSION AND RECOMMENDATIONS

7.0 Introduction

This chapter contains the general discussion of how this proposed solution compares with what exists currently, future recommendations to further enhance this solution and concluding remarks about the research undertaken.

7.1 General Discussion

Mobile payment is a real revelation to the Kenyan economy; it is in use nearly in all aspects of the Kenyan economy from paying school fees, to hospital bills and utility bills. The mobile industry has grown in leaps in bounds since the introduction of the first mobile operator in the country which was Kencell now Airtel Kenya. From that time hence forth the prices of the handsets has reduced drastically making it affordable even to the ordinary mwananchi who during the inception years of the mobile industry could not afford the handsets. This has greatly increased the number of mobile users in the country. Through research, many mobile operators have formulated new ideas on rolling out services to their subscribers like through the use of Airtel money, M-Pesa and of late M-shwari which was launched by Safaricom on 21st November 2012. Through these applications especially M-pesa has seen a lot of people prefer the mobile payment option than opposed to the norm of using banks or carrying hard cash. Mobile payment is relatively safe as it helps one to transfer money even to people who are far away, the

only thing needed is one to be a registered mobile payment user, have a handset and be near an agent in case one needs to deposit or withdraw money.

The issue of non-repudiation and fraud has been one of the main blocks that have been blocking the growth of this sector. Fraudsters are constantly finding new ways of stealing money from people who use these mobile payment applications. The ways vary from masquerading as mobile operator customer service people and ask people to input a certain code through their mobile payment service and from there they have access to your mobile payment account, sending false messages of transactions purporting to have been carried out between you and them, stealing people's PIN. Those are some of the most common ways of fraud been conducted on mobile payment applications. The mobile operators are constantly researching for new means of ensuring these incidents of fraud and non-repudiation do not occur on their platforms and one way is they have included campaigns that urge their users to keep safe their PIN numbers and never reveal them to anyone.

The PIN mechanism has various algorithms that are used to generate and verify the PIN that was entered by the user. But there is no algorithm that sought to enhance PIN to provide non-repudiation. The major PIN algorithm is the IBM algorithm. This algorithm catered for the generation and verification of the PIN entered by the users but did not seek to answer on the question of non-repudiation.

During the course of the project, one aspect was to come up with an algorithm that would seek to combine the two mechanism that is the PIN and timestamps in order to have an effective non-repudiation mechanism for the proposed security enhancement

which would enable PIN not only to act as an authorization mechanism but also be able to provide non-repudiation.

This research project set out to answer one major objective, whether it was possible to enhance PIN to provide non-repudiation through the use of timestamps. The mode of application with which to test the mentioned objective was to develop a mobile payment application which would authorize transactions through use of the PIN which was provided by the user. The application would check the PIN provided against the one stored in the database, compare the two and if it was the correct PIN, it would authorize the transaction otherwise it would reject the transaction.

An evaluation of the current mobile payment systems and banking applications revealed that it is necessary to ensure that non-repudiation mechanisms are present in all the applications that tend to deal with financial matters and time was noted to be of upmost importance in the assurance that the applications catered for the security of the transactions. Most of these applications have implemented secure mechanism to protect their consumers from fraud and thus up to speed with the need for secure applications.

7.2 Evaluation

In this study one of the aspects needed to be investigated was how many people especially business owners would use mobile payment in their businesses to transact. After data was collected and analyzed it was clear that most of the respondents who participated in the study would agree to transact with their customers through mobile payment applications but only if there was mutual trust between the two. This is true in relation to the 3rd quarter data for June 2012 of the CCK which clearly showed that

people had a lot of faith in these mobile payment applications. From the data collected in the study, it showed that a lot of the respondents had knowledge of the PIN and timestamp mechanism. From the analysis done it helped a lot in the formulation of the system design of the proposed mobile payment application that would in turn test the formulated implementation of the proposed algorithm.

The algorithm deduced in the systems design phase and the subsequent UML diagrams portraying the system flow of the proposed application helped much in testing the major objective of the project. The outstanding aspect of my proposed enhancement of PIN to provide non-repudiation through timestamps were tested during the experiment phase of the project and in the conclusion part are the things noted during the experiment phase.

Algorithm PIN Time stamp Generation (PIN, Payer number, payee number, System Time)

NRO AND
NRR services
represented in
steps 1 to 7 of
the algorithm

Step1: Define SIZE: (size of the PIN length)

Step2: Find numbers of payer and payee.

Step3: Check numbers if they are registered for the service in the database

Step 4: if (Payer number and Payee number= Stored Numbers)

They are registered for the service

Else Terminate request

Step 5: Count Number of Characters of the PIN (Integer)

Step 6: Is it the correct PIN

Step 7: if (Count = Size) and PIN=Stored PIN

Correct Input and ready for authorization of transaction

Else return Wrong PIN;

NRT service
represented
from step 8 to
11 of the
algorithm

Step 8: Date/Time of Transaction is sought through use of the system time of the machine running the application.

Step 9: Transaction Id, Date/Time, Payer and Payee numbers, amount and PIN are counter checked before request is committed and stored in the in_msg table stored in the database.

Step 10: The Payer and Payee numbers, Transaction Id, amount and Date/Time of transaction being stored as in the out-msg table.

Step 11: Send message with confirmation of the payment request

Using this algorithm the application is able to verify the correctness of the PIN, the time the transaction was effected together with the transaction ID and also the storage of the correct log which shall be used in case fraud or a case crops up. The above algorithm corresponds for Non-repudiation of Origin (NRO) , Non Repudiation of Transit and Non Repudiation of Receive (NRR) where the whole request is checked whether its' correct and timestamp added to it to indicate the time it was done. NRO and NRR are done in steps 1 to 7 in the algorithm. This is where the details of both parties are verified before the request is done. NRT is done in steps 8-11 of the algorithm where the timestamp details are effected into the transaction request and are stored in the out_msg(out message table in the database).

7.3 The Enhanced Parts Of The Algorithm

The main purpose of this research project was to enhance pin to provide non-repudiation through use of timestamps. The proposed algorithm above contains various enhancements which shall be explained below:

1. Currently there exists no algorithm for PIN to provide non-repudiation, the only ones available are for PIN generation, PIN validation and PIN offset algorithms all by IBM. The main aspect was to enhance PIN to provide non-repudiation through use of timestamps. The algorithm in step 5, 6, 7 ensures that the PIN entered to authorize the transaction request is the correct PIN (this is evident in current applications/ algorithms in use today to authorize transactions). After they have been verified the time of the request is noted from the system time of the machine running the application (in step 8). Then the time is appended to the details of the transaction request which include the numbers involved and the authorizing PIN. The time is noted when the PIN used for authorization has been verified and the request is being processed. Here the receiving time of the request and the sending time of the details pertaining to the two transactions are formulated through use of the system time of the machine. This time will be used to show the time the request was sent and finalized. As stated at the start of the project, this research will not deal with generating PIN's but on enhancing them to provide non-repudiation. The stated steps are the enhancement of the algorithm where in most applications, the authorization part is done separately

from the non-repudiation parts. In the enhancement both the authorization and non-repudiation are done together.

2. For non-repudiation to be ensured in financial applications, it is very important to ensure that only registered persons/ authenticated person use the service. Good examples are bank ATM's where only persons who hold bank accounts and have registered to have ATM service use that service. Previously, most mobile payment applications allowed anyone to use their service as long as you're on their network; this created a lot of problems especially with fraud. And with the on-going subscriber registration initiative to curb these cases, the mobile service subscribers can improve by only allowing subscribed users to their mobile payment service to use that application. One of the enhancements of the algorithm to check if the people using the application are registered enhances security of the application. This is evident in step 2, 3, 4 of the algorithm.

7.4 Compared To Existing Approaches

Current mobile payment applications ensure atomicity of the transactions, in the proposed enhancement of the algorithm, atomicity is ensured entirely from the moment the numbers and PIN used in the request are verified. This is different from current approaches which take only when the request is being processed or after processing. The enhancement ensures that before the request is processed, the time the details were sent, the time is noted down. This is the NRT part of the algorithm. The enhanced algorithm provides two distinct times, that is the time the request was sent and the time it finalized the transfer of amounts to the respective parties.

The proposed algorithm enhances PIN to provide non-repudiation through the use of timestamps. This enhancement is clearly shown in the algorithm from steps 5 to 8 of the algorithm. In the formulation of the timestamps, the timestamp should be reliable and thus the Time Stamping Authority in this case the system time should be correct and be acceptable to both parties. Compared to what has been done, the enhanced parts of the algorithm explained above ensure non-repudiation of the transactions. The PIN enhancement through use of the timestamps increases the capability of PIN to provide non-repudiation. Current mobile payment applications enforce atomicity of the transactions also through use of timestamps, the enhanced parts of the algorithm ensure that the atomicity of the PIN is enforced on a real-time basis; this ensures that the time the PIN is authorized is also the same time the request will be processed. The details will be stored in the database which shall be accessible by authorized users.

The second enhancement of the algorithm ensures that only registered users use the service. The steps 2, 3, 4 ensure that only registered users use the service. This further enhances the non-repudiation aspect of this algorithm that ensures that non-registered people don't use the service. Also this part ensures if one entered a wrong PIN the request will not be processed. Compared to existing approaches in use today, current mobile payment applications allowed people to receive money even if they were not registered to use the service. No mechanism or application will be without repudiation cases if un-registered/un-known people use their applications.

7.5 Conclusion

In conclusion the algorithm that was proposed in the design stage of the project helped in enhancing PIN to provide non-repudiation through the use of timestamps. The time stamps were generated through the system time which was captured when the request was received by the application and the processed. This request contained the payment information which is the PIN, amount, and number of the person whom the payment is made to. The PIN is used to authorize the transaction.

7.6 Recommendation

1. The use of timestamps as a means of non-repudiation through use with PIN will aid significantly in the fight against repudiation of transactions by people, through the proposed algorithm it ensures that only registered persons are able to transact through the mobile payment application. Also the novelty of enhancing PIN to provide non-repudiation can be further enhanced by use of digital signatures in these applications or by use of biometrics.
2. The only remaining part of the proposed security is when being implemented is that it did not cater for the saving of the payment requests that were being done. This is because the application would keep on checking or waiting for incoming request , and because these request are stored in the in_msg table in the database, the application kept on redoing the request that had already being done. Hence the details of the incoming requests were processed immediately and not stored

in the `in_msg` table so as to prevent the same request being redone over and over again. That is the only aspect of the proposed security feature that needs future work.

REFERENCES

1. A.Cenys, A. Normantas and L. Radvilavicius (18 May 2009), “*Designing role-based access control policies with UML*” Information Security Laboratory, Department of Information System, Faculty of Fundamental Sciences.
2. Agarwal, S., Khapra, M., Menezes, B., & Uchat, N. Security Issues in Mobile Payment Systems. *Indian Institute of Technology, Bombay, India*. 2007. (Pg 2)
3. Bonnecaze, A., Liardet, P., Gabillon, A., & Blibech, K. (2006, June). Secure time-stamping schemes: A distributed point of view. In *Annales des télécommunications* (Vol. 61, No. 5-6, pp. 662-681). Springer-Verlag.
4. Boneh, D., Ding, X., Tsudik, G., & Wong, C. M. (2001, August). A Method for Fast Revocation of Public Key Certificates and Security Capabilities. In *USENIX Security Symposium* (pp. 22-22).
5. *C# standard*, <http://www.ecma-international.org/publications/standards/Ecma-334.htm>
6. Cattan, A, and Tomer B. (2005) "Web development and deployment using SMS and USSD." U.S. Patent No. 6,961,330.

7. Caulfield, H. J., & Halter, E. (2002). *U.S. Patent No. 6,421,943*. Washington, DC: U.S. Patent and Trademark Office.
8. Clarke, N. L., & Furnell, S. M. (2005). Authentication of users on mobile telephones—A survey of attitudes and practices. *Computers & Security*, 24(7), 519-527.
9. Chen, B., Cheng, H. H., & Palen, J. (2006). Mobile-C: a mobile agent platform for mobile C/C++ agents. *Software: Practice and Experience*, 36(15), 1711-1733.
10. Clulow, J. S. (2003). The design and analysis of cryptographic APIs for security devices
11. Coffey, T., & Saidha, P. (1996). Non-repudiation with mandatory proof of receipt. *ACM SIGCOMM Computer Communication Review*, 26(1), 6-17.
12. Debbai, M. Saleh, M. Talhi and C. Zhioua (2005). Security analysis of mobile Java. In Proceedings of Sixteenth International Workshop on Database and Expert Systems Applications. pp. 231- 235.
13. D. Kugler (2003). Man in the Middle Attacks on Bluetooth. In Financial Cryptography '03, Long Beach. Lecture Notes in Computer Science, Springer-Verlag.

14. E.Barkan, E. Biham, and N. Keller (2006). Instant Cipher text-Only Cryptanalysis of GSM Encrypted Communication. Technion-Computer Science Department - Technical Report CS-2006-07.

15. Funk, J. L. (2005). *The future of the mobile phone Internet: an analysis of technological trajectories and lead users in the Japanese market*, Technology in Society, Vol. 27 (1), 69-83

16. Fischer, M., Gall, H., & Hauswirth, M. (2002). *Towards a generalized payment model for Internet services*. University of Vienna, pp 81-90.

17. Gritzalis S., Iliadis J., Gritzalis D., Spinellis D., and Katsikas S. (1999), "Developing Secure Web-based Medical Applications", Medical Informatics journal, Cambridge University Press - Taylor & Francis Publics, Vol.24, No.1, pp.75-90.

18. Haber, S., & Stornetta, W. S. (1997, April). "Secure names for bit-strings". In *Proceedings of the 4th ACM Conference on Computer and Communications Security* (pp. 28-35). ACM.

19. Haber, S., & Stornetta, W. S. (1991). *How to time-stamp a digital document* (pp. 437-455). Springer Berlin Heidelberg.

20. Gavalas, D., & Economou, D. (2011). Development platforms for mobile applications: Status and trends. *Software, IEEE*, 28(1), 77-86.

21. Hughes, N., & Lonie, S. (2007). M-PESA: mobile money for the “unbanked” turning cellphones into 24-hour tellers in Kenya. *Innovations*, 2(1-2), 63-81.

22. IBM PIN generation algorithm

[http://www.ibm.com/3624 pin geneation.html](http://www.ibm.com/3624%20pin%20geneation.html)

23. IBM PIN offset algorithm

[http://www.ibm.com/pin offset generation.html](http://www.ibm.com/pin%20offset%20generation.html)

24. IBM PIN validation algorithm

[http://www.ibm.com/3624 pin verification.html](http://www.ibm.com/3624%20pin%20verification.html)

25. Implementing non-repudiation- Docs Oracle

http://docs.oracle.com/cd/E13214_01/wli/docs70/b2bsecur/nonrep.htm

26. International Organization for Standardization, ISO Standards ISO/IEC 13888-1:2009, Information technology- Security Techniques-Non-Repudiation- Part 1: General Introduction <http://www.iso.org>

27. International Organization for Standardization, ISO Standards ISO/IEC 13888-2:2009, Information technology- Security Techniques-Non-Repudiation- Part 2: Mechanisms using symmetric techniques <http://www.iso.org>
28. International Organization for Standardization, ISO Standards ISO/IEC 13888-3:2009, Information technology- Security Techniques-Non-Repudiation- Part 3: Mechanisms using asymmetric techniques <http://www.iso.org>
29. Java Community Process: JSR-000177 Security and Trust Services API for J2ME. (Online)
<http://jcp.org/aboutJava/communityprocess/final/jsr77/>.
30. Keynote, White Paper on "Testing Strategies and Tactics for mobile Applications".
http://www.keynote.com/docs/whitepaper/WP_Testing_Strategies.pdf
31. Kastner, C., Thum, T., Saake, G., Feigenspan, J., Leich, T., Wielgorz, F., & Apel, S. (2009, May). FeatureIDE: A tool framework for feature-oriented software development. In *Software Engineering, 2009. ICSE 2009. IEEE 31st International Conference on* (pp. 611-614). IEEE.
32. Kothari, C. R. (2009). *Research methodology: methods and techniques*. New Age International.

33. Kuhn, D. R., Hu, V. C., Polk, W. T., & Chang, S. J (2001). *Introduction to public key technology and the federal PKI infrastructure..* NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD. (Pg 8)
34. L.Carettoni, C.Merloni and S. Zanero (2007). “Studying Bluetooth Malware Propagation: The BlueBag Project”. IEEE Security & Privacy Vol. 5, 2.
35. Mas, I., & Morawczynski, O. (2009). Designing mobile money services lessons from M-PESA. *Innovations*, 4(2), 77-91.
36. Merkle, R. C. (1990, January). A certified digital signature. In *Advances in Cryptology—CRYPTO’89 Proceedings* (pp. 218-238). Springer New York.
37. Mobile Payments in M-Commerce, White paper. (2002). Retrieved November 11, 2011, from Cap, Gemini, Ernst and Young Web site: <http://www.cgey.com/tmn/pdf/mobilePaymentsinMCommrce.pdf>
38. Mugenda, O. & Mugenda A. (1999). *Research Methods: Quantitative & Qualitative Approaches*. Acts Press, Nairobi, pp 50-51, 115-130.
39. N. -J. Park and Y. -J. Song, (2001) "M-Commerce security platform based on WTLS and J2ME," presented at Industrial Electronics. IEEE International Symposium.

40. Paybox: ePSO Inventory Database (n.d.). Retrieved November 01, 2011, from <http://www.e-pso.info/epso/index.html>
41. Paybox.net. (2001). Paybox security, Whitepaper, business and technical information regarding the security at paybox. Retrieved November 01, 2011, from http://www.paybox.net/publicrelations/public_relations_whitepapers.html
42. Paybox.net. (2002). Mobile commerce delivery made simple: Whitepaper. Retrieved November 01, 2011, from http://www.paybox.net/publicrelations/public_relations_whitepapers.html
43. Royce, Winston (1970), "Managing the Development of Large Software Systems", *Proceedings of IEEE WESCON 26* (August): 1–9,
44. S. Fong and E. Lai (2005). Mobile Mini-payment Scheme Using SMS-Credit. International Conference on Computational Science and Its Applications-ICCSA. pp. 1106-1114.
45. S. F. Mjølsnes and C. Rong, (2003.) "*On-line e-wallet system with decentralized credential keepers,*" *Mobile. Network. Appl.*, vol. 8, pp. 87--99,
46. Sector statistics report Q3 June 2012 Communications Commission of Kenya.

http://www.cck.go.ke/resc/downloads/SECTOR_STATISTICS_REPORT_Q3_JUNE_2012.pdf

47. Sector statistics report Q2 2011/2012 Communications Commission of Kenya.

http://www.cck.go.ke/resc/downloads/SECTOR_STATISTICS_REPORT_Q2_2011-12.pdf

48. Sommerville, I. (2004). 7th Edition, *Software Engineering*. Dorling Kindersley, India, pp 139-162.

49. Standard ECMA-334 (2006) - C# Language Specification, C# Standard. "334." ISO/IEC 23270.

50. Stuart Haber, W. Scott Stornetta (1991) "*How to Time-stamp a Digital Document*" Lecture Notes in Computer Science", Vol. 537,

51. Technology and development: The real digital divide | *The Economist*

<http://www.economist.com/node/3742817>

52. Tiwari, Rajnish and Buse, Stephan (2007): "*The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector*". Hamburg University Press

APPENDIX

Appendix 1: Questionnaire for business owners

QUESTIONNAIRE: ENHANCING PIN TO PROVIDE NON-REPUDIATION IN MOBILE PAYMENT APPLICATIONS.

FOR MOBILE PAYMENT USERS: - BUSINESSES

This questionnaire will help me the researcher to know the security challenges affecting mobile payment transactions, perception of users towards these mechanisms used to provide secure payment options for them and how aware are the users on the various mechanisms in use to provide authorization and non-repudiation.

Non-repudiation: ensures if two or more parties are involved in transaction, no party can dishonor the transaction be it in the form of refusal to commit payment, unlawful statement of payment (that is a party purporting to have done the payment while in actual sense no payment was done by the said party).

PIN: Personal Identification Number Mechanism. It used to authorize transactions in a mobile payment application. Usually a number digit one inputs before the transaction is authorized.

Authorization: The act of ensuring only the owner of the mobile phone on which the application/system is running can effect a transaction.

Repudiation: The act of one party either dishonoring/failing to commit to the transaction with which they had agreed with another party.

Digital Signatures: is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document/ transaction.

Biometric authorization: a type of security authorization based on human part inputs example finger print identification in order to authorize a transaction.

Time stamping: A timestamp is the current time of an event that is recorded by a computer

Secure audit logs: is a security-relevant chronological record, set of records, or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.

QUESTIONNAIRE NUMBER:

Category 1: Demographic information on those who use mobile payment applications

1. Education level? Primary Secondary Tertiary/university/college

2. Gender? Male Female

3. Age _____

4. Do you use mobile payment in your business? Yes No

If no in question 5, please explain why

.....
.....
.....
.....

5. Experience in using a mobile payment application?

No experience

Novice user

Advanced/expert user

CATEGORY 2: Users awareness and perceptions towards authorization and non-repudiation mechanisms

6. Which of the following authorization and non-repudiation mechanism do you know?

Mechanisms For authorization	Please tick which you know
Pin(Personal Identification Number)	<input type="checkbox"/>
Biometrics	<input type="checkbox"/>
Digital Signatures	<input type="checkbox"/>
Passwords and User Accounts	<input type="checkbox"/>

MECHANISM FOR NON-REPUDIATION

Mechanism for Non-repudiation	Please tick which you know
Time stamping	<input type="checkbox"/>
Digital Signatures	<input type="checkbox"/>
Secure logs	<input type="checkbox"/>

7. What security precautions do you take to ensure that your customers do not fault on their transactions?

.....

.....

.....

.....

8. Have you ever had a repudiated transaction with a person whom you were transacting with through these applications?

Yes No

If Yes in question 8, explain how the case was able to be resolved, if the case was resolved

.....
.....
.....
.....
.....
.....

9. Please tick your response based on your view pertaining to the following statements. Key SD- Strongly Disagree; D- Disagree; N- Neutral; A- Agree; SA- Strongly agree .Please tick where appropriate

Category 3: Security Challenges Facing Mobile Payment users

	SD	D	N	A	SA
The current non-repudiation mechanisms employed in mobile payment applications ensure the transactions are safe.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Current mobile payment applications provide good non-repudiation mechanism to protect you against repudiation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Current mobile payment applications are very secure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

10. What are the security challenges you encounter while doing money transfer through the mobile payment applications?

.....

.....

.....

.....

.....

.....

.....

11. What Security measures/mechanism would you like to be added to mobile payment applications in order to ensure the security challenges are mitigated?

.....

.....

.....

.....

.....

Appendix 2: Questionnaire for Mobile Service Providers

QUESTIONNAIRE: ENHANCING PIN TO PROVIDE NON-REPUDIATION IN MOBILE PAYMENT APPLICATIONS. FOR MOBILE SERVICE PROVIDERS

This questionnaire will help me the researcher to know the views of the mobile service providers on the challenges their applications face, what they have done to mitigate these challenges and also get to know the technical aspects involved in developing such applications.

Non-repudiation: ensures if two or more parties are involved in transaction, no party can dishonor the transaction be it in the form of refusal to commit payment, unlawful statement of payment (that is a party purporting to have done the payment while in actual sense no payment was done by the said party).

PIN: Personal Identification Number Mechanism. It used to authorize transactions in a mobile payment application. Usually a number digit one inputs before the transaction is authorized.

Authorization: The act of ensuring only the owner of the mobile phone on which the application/system is running can effect a transaction.

Repudiation: The act of one party either dishonoring/failing to commit to the transaction with which they had agreed with another party.

Digital Signatures: is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document/ transaction.

Biometric authorization: a type of security authorization based on human part inputs example finger print identification in order to authorize a transaction.

Time stamping: A timestamp is the current time of an event that is recorded by a computer

Secure audit logs: is a security-relevant chronological record, set of records, or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.

QUESTIONNAIRE NUMBER:

Category 1: Demographic information

1. Company Name _____

2. Education level? Primary Secondary Tertiary/university/college

3. Gender? Male Female

4. Age

5. Position held in the Company _____

Category 2: Technical aspect of the mobile payment system in use

6. What are the various non-repudiation and authorization mechanisms used in your mobile payment system?

Mechanisms For authorization	Please tick which you know
Pin(Personal Identification Number)	<input type="checkbox"/>
Biometrics	<input type="checkbox"/>
Digital Signatures	<input type="checkbox"/>
Passwords and User Accounts	<input type="checkbox"/>

MECHANISM FOR NON-REPUDIATION

Mechanism for Non-repudiation	Please tick which you know
Time stamping	<input type="checkbox"/>
Digital Signatures	<input type="checkbox"/>
Secure logs	<input type="checkbox"/>

If there is any other mechanism in use for either authorization or non-repudiation please specify

.....

.....

.....

.....

.....

7. What has been done to try and enhance PIN to provide non-repudiation in today's mobile payment applications?

.....

.....

.....

.....

.....

8. What are the security challenges facing people who transact through mobile payment applications?

.....

.....

.....

.....

.....

.....

9. How do you handle repudiation cases that occur in mobile payment application (procedure in handling repudiation cases)?

.....

.....

.....

.....

.....

10. How do you store these transaction details in the database?

.....

.....

.....

.....

.....

11. Do you also store the information provided by the authorization and non-repudiation mechanisms you put in place in your applications?

.....

.....

.....

.....

.....

12. Do you store the transaction details and information provided by the security mechanisms in the same repository/ database?

.....

.....

.....

.....

.....

13. How will this information be retrieved from the database?

.....

.....

.....

.....

.....

.....

14. How do you ensure that the transaction details you store in your databases are secure from outside intrusion or tampering?

.....

.....

.....

.....

.....

15. How is the evidence achieved and presented from the system itself for such cases mentioned above.

.....

.....

.....

.....

.....

16. Which application development platform do you prefer to be used in developing mobile payment application?

.....
.....
.....
.....
.....
.....

17. What added security feature would you find best for a mobile application that will be developed so that it ensures strong authorization and non-repudiation protocols?

.....
.....
.....
.....
.....
.....

	SD	D	N	A	SA
<p>18. Would enhancing PIN with time stamps in order to enable PIN to provide non-repudiation be a good solution for the problem of repudiation.</p> <p>(Please tick where appropriate)</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

THANK YOU