



UNIVERSITY OF NAIROBI
SCHOOL OF COMPUTING AND INFORMATICS

DATA CAPTURE MODEL FOR UTILITY PROVIDERS USING
HAND HELD DEVICES VIA MOBILE NETWORK: CASE FOR
NAIROBI WATER COMPANY

BY

P56/P/8887/2006: KIPLAGAT DAVID

October 2008

Submitted in partial fulfillment of the requirements of the degree of Masters of Science in
Computer Science

University of NAIROBI Library




0525356 2


DECLARATION

This Project, as presented on this report is my original work and to the best of my knowledge has not been presented for any other university award.

Signed: 
David Kiplagat, P56/P/8887/2006

Date: 

This Project has been submitted as part of fulfillment of the requirements for the award of Masters of Science in Computer Science of the School of Computing and Informatics of the University of Nairobi, with my approval as the University Supervisor.

Signed:  School of Computing & Informatics
University of NAIROBI
P. O. Box 30197
NAIROBI

Date: 

ACKNOWLEDGMENTS

I wish to express my sincere appreciation to Dan Orwa, my supervisor, for his invaluable counsel and guidance towards the successful completion of this research project, and indeed for his immense assistance all through this MSc. course. Special thanks also to all my MSc lecturers for sharing their knowledge with me during this last year. Thanks also to my colleagues for their valuable input.

I wish to also express my sincere acknowledgement to Nairobi Water Company (NWSC) staff for conducting the usability test and filling the questionnaire. Special thanks goes to Grace Ndungu the HR manager (NWSC) for granting me the authority to carry out research, the Billing Manager Josiah Gitu (NWSC) who assisted me to get the participants to carry out the test, the training and change management coordinator (NWSC) Peter Kamau Mwangi for seeing into it that my request to conduct research was granted and above all Lenah Ngungu the Billing Officer (Central Region-NWSC) who was in charge of the participants that tested the system and filled the questionnaire.

I owe my deepest appreciation and gratitude to Mr. M. Mukiiri, Mr. P. Kariuki and Mrs. J. Mwangi for assisting me in the configuration and installation of the development environment. I would also like to extend a special thank you to Mr. Peter Cech a kannel expert for assisting me in getting configuration file working after trying for more than one month.

In addition, I owe thanks to the rest of my family: my son, Denley, my wife Angeline and the rest of my extended family and friends. You have all provided me with love and inspiration. Thank you.

DEDICATION

Special dedication goes to my son Denley Kipkoech Lagat and my lovely wife
Angeline Kiplagat.

PERMISSION TO LEND AND/OR COPY

*I agree that University of Nairobi Library may lend or copy this Research
Project upon request.*

Signed: 

David Kiplagat.

October 2008.

ABSTRACT

Utility providers faces a major task of collecting data from there remote installations. In order to be more efficient there is a growing need to reengineer there operations to make them more efficient, effective and customer focused while reducing the cost of operation both in terms of personnel involved, time and the actual operational costs. With the current emergence of 3G networks in wireless network there is need for this companies to look closely at mobile computing as the most cost effective solution to fix there problems.

This research project mainly targeted the utility providers and the focus was to come up with a cost effective, secure, usable, adaptable, portable and above all extensible mobile data collection model and implement it as a prototype system that can be combined with other e-enabling technologies to create a holistic system for utility providers to reengineer there current business processes to make them more efficient and effective thereby improving on customer perception.

Using the WAP model has the preferred technology, this research as added to the voices of WAP proponents who have been suppressed by the opponents by proposing a solution to solve the current major problem of WAP, lack of end to end security which its opponents have used has a weapon to discredit the WAP technology. This has been done by using the kannel Gateway which can be configured within the web server of the organization hence no need of an external provider.

Also this research as shown that there is actually no need to acquire other devices to enhance on meter reading. The mobile phones can be used to achieve a lot. If the recommended further work can be pursuit it can be seen that the capabilities of mobile phones are enormous and can actually transform the way companies conduct there business.

List of Figures

Figure 1.1: WWW Model	7
Figure 1.2 WAP	8
Figure 1.3 WAP Protocol Stack	9
Figure 1.4 WAP Model Security Analysis	10
Figure 1.5 WAP Security Loop Hole	10
Figure 1.6 SMS Model	14
Figure 1.7 Secure SMS Model	16
Figure 1.7 Secure SMS Protocol Stack	18
Figure 1.8 The Structure of a Secure SMS Message	21
Figure 1.9: AMR Solution	23
Figure 2.0: UAS System Technical schematic diagram	28
Figure 2.1 Kannel WAP and SMS Gateway architecture	31
Figure 2.2 Solution to the WAP gap	31
Figure 2.3 Mobile data collection model	35
Figure 2.4 Workflow of the manual process	36
Figure 2.5 Workflow of the PDA logger Process	39
Figure 2.6 Workflow of the proposed solution	50
Figure 2.7 Modules interaction	51
Figure 2.8 Device Adapter Module	52
Figure 2.9 Flow Chart Authentication Module	54
Figure 3.0 Meter Reading Module Design	55
Figure 3.1 SMS Data flow diagram	56
Figure 3.2 Flow Chart of the proposed Prototype Design	57
Figure 3.3 Meter Reading Module Database Design	57
Figure 3.4 Administrative Menu Database Design	58
Figure 3.5 SMS Messaging Module Database design	59
Figure 3.6 Customer Monthly Statements Database Design	60
Figure 3.7 Device Adapter Module Functional Representation	65
Figure 3.8 Meter Reading Module Prototype	67
Figure 3.9 Simulation Testing of the prototype	71
Figure 4.0 Simulation to show adaptability of the prototype	72
Figure 4.3 human information processing of the product interface	85
Figure 4.4 a framework for usability testing of data collection system	87
Figure 4.5 Average time taken to complete a transaction	91
Figure 4.6 Graph showing comparison of means and standard deviation of all variables	94
Figure 4.7 Model Security Analysis	97
Figure 4.8 VPN Network	100

List of Tables

Table 1.1 Manual process analysis -----	37
Table 1.2 Logger process analysis-----	40
Table 1.3 the average completion time in seconds taken by each participant-----	90
Table 1.4 the means and standard deviations of all variables-----	93
Table 1.5 cronbach's alpha test of different dimensions-----	40

Terminology

AMR	Automatic Meter Reading System
3G	Third Generations wireless network
API	Application Program Interface
BSC	Base Station Controller
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
DCS	Data Collection Systems
GMSC	Gateway Mobile Services Controller
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
GUI	Graphical User Interface
HLR	Home Location Register
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
IT/IS	Information Technology/ Information System
J2ME	Java 2 Platform, Micro Edition
KPLC	Kenya Power and Lighting Company
MIDlet	Mobile Information Device Application
MSC	Mobile Services Switching Centre
MSISDN	Mobile Station International PSTN/ISDN Number
MSRN	Mobile Station Roaming Number
NWC	Nairobi Water Company
PAP	Push Access Protocol
PC	Personal Computer
PI	Push Initiator
UP	Utility Provider
SMS	Short Message Service
SMS-C	Short Message Service Centre
SNMP	Simple Network Management Protocol
SMPP	Short Message Peer to Peer Protocol
TCP/IP	Transport Control Protocol/ Internet Protocol
WAE	Wireless Application Environment
WAP	Wireless Application Protocol
WDP	Wireless Datagram Protocol
WGP	WAP Gateway Proxy
WML	Wireless Markup Language
WSP	Wireless Session Protocol
WTP	Wireless Transaction Protocol
WTLS	Wireless Transport Layer Security
WWW	World Wide Web
XHTML	eXtensible HyperText Markup Language
XML	eXtensible Markup Language
RADIUS	Remote -Authentication Dial-In User Service; an AAA server

TABLE OF CONTENTS

ACKNOWLEDGMENTS	ERROR! BOOKMARK NOT DEFINED.
DEDICATION.....	ERROR! BOOKMARK NOT DEFINED.
PERMISSION TO LEND AND/OR COPY	VI
ABSTRACT.....	VII
LIST OF FIGURES.....	VIII
LIST OF TABLES.....	IX
TERMINOLOGY	I
TABLE OF CONTENTS.....	1
CHAPTER 1: INTRODUCTION.....	3
1.1 BACKGROUND INFORMATION	3
1.2 OUTLINE OF THE REPORT.....	4
1.3 PROBLEM DESCRIPTION	4
1.4 PROJECT JUSTIFICATION/MOTIVATION	5
1.5 RESEARCH QUESTIONS	6
1.6 OBJECTIVES.....	6
1.7 PROJECT SCOPE	7
CHAPTER 2: LITERATURE REVIEW	8
2.1 BACKGROUND INFORMATION	8
2.2 MOBILE DATA COLLECTION MODELS.....	8
2.2.1 <i>The World Wide Web model</i>	8
2.2.2 <i>WAP MODEL</i>	10
2.2.3 <i>SMS Model</i>	14
2.2.4 <i>Secure SMS Model</i>	17
2.3 EXISTING MOBILE DATA COLLECTION SYSTEMS	22
2.4 ENABLING TECHNOLOGIES.....	27
2.5 THEORETICAL RESEARCH MODEL.....	31
CHAPTER 3: METHODOLOGY.....	36
3.1 ANALYSIS.....	36
3.1.2 <i>Overview</i>	36
3.1.3 <i>Methodology used</i>	36
3.1.4 <i>Requirement Analysis</i>	37
3.2 DESIGN.....	50
3.2.1 <i>Prototype Design</i>	50
3.2.2 <i>Detailed Design of the prototype</i>	53
3.2.3 <i>Device Adapter Module</i>	53
3.2.4 <i>Authentication Module</i>	54

3.2.5	<i>Meter Reading Module</i>	57
3.2.6	<i>SMS Messaging Module</i>	57
3.2.7	<i>PDF Generator Module</i>	58
3.2.8	<i>Emailing Module</i>	58
3.2.9	<i>Database Design:</i>	60
CHAPTER 4: PROTOTYPE IMPLEMENTATION		63
4.1	OVERVIEW	63
4.2	CHOICE OF TECHNOLOGIES USED	63
4.3	SETTING THE DEVELOPMENT ENVIRONMENT	64
4.4	DEVELOPMENT OF THE PROTOTYPE	67
4.4.1	<i>Device adapter Module</i>	67
4.4.2	<i>Meter Reading Module</i>	67
4.4.3	<i>SMS Messaging Module</i>	70
4.4.4	<i>Emailing Module</i>	70
4.4.5	<i>PDF Generator Module</i>	72
4.4.6	<i>Administrative Module</i>	72
4.5	SIMULATION AND EVALUATION OF THE PROTOTYPE	73
4.6	USABILITY ANALYSIS	74
4.7	SECURITY ANALYSIS	85
4.7.1	<i>Security threats</i>	86
4.7.2	<i>Security Analysis of mobile data collection system</i>	87
CHAPTER 5: DISCUSSION AND RECOMMENDATION		94
5.1	INTRODUCTION	94
5.2	SUMMARY OF RESEARCH PROJECT	95
5.3	ACHIEVEMENTS	95
5.4	LIMITATIONS AND CHALLENGES	97
5.5	SUGGESTED FURTHER RESEARCH:	98
5.6	CONCLUSIONS	99
REFERENCES:		100
APPENDIX A: KANNEL CONFIGURATION FILES		102
APPENDIX B: KANNEL INSTALLATION		105
	DOWNLOADING AND COMPILING	105
	RUNNING THE SERVER	105
APPENDIX C: PROTOTYPE USER MANUAL		106
APPENDIX D: CODE SAMPLES		113
APPENDIX E: USABILITY ANALYSIS EXPERIMENT AND QUESTIONNAIRE		114

Chapter 1: Introduction

1.1 Background Information

Companies providing utility services like water and electricity face uphill task of reading meters monthly and updating their customers' records for monthly billing. The Nairobi Water Company (NWC) in particular is loosing millions of shillings monthly for its unreliable meter reading and onward updating of customers records. It takes up to two months to get bills after meter reading mainly as a result of slow data entry and also prone to so many errors. A lot of man hours are wasted in sorting out billing problems that could have been easily avoided.

With the emergence of mobile communication and so many protocols to offer connectivity via the mobile network, remote connectivity can be achieved from anywhere covered by mobile network. To solve this problem there is need for these companies to utilize the GSM network which covers the entire city of Nairobi and most parts in Kenya to connect to the their databases such that data from the meter reading can be fed directly from the source using hand held devices.

One technology for implementing data collection services is WAP, short for Wireless Application Protocol. It lets the phone act as a simple hypertext browser, but optimizes the markup language, scripting language, and the transmission protocols for wireless use. The optimized protocols are translated to normal Internet protocols by a WAP gateway.

In this Project a data collection and secure customer care prototype system based on Nairobi City Water & Sewerage Company LTD (NWC) will be developed using the WAP gateway technology. This will also eliminate a third party which mainly offers getaway link.

The meter reader will be required to have a WAP enabled phone. The meter readers will just like the way they do normally, visit a premise logs into the company system via the mobile phone through a web interface developed for the purpose but customized to run on the limited capabilities of a mobile phone. He then enters the ID of the customer and the current meter reading. The customers' statement will be updated immediately and send as a PDF document to the customers email account also the customer can query for balance via the SMS which is also provided for by the system. This will enable the utility companies

to fully utilize the services of the meter readers and be prompt thereby increasing the revenue and efficiency.

Apart from development of the prototype this project will try to highlight the capability of mobile phone as a capable information device. We shall also investigate how secure is the technology we are adopting.

1.2 Outline of the Report

This research project contains five main chapters. First there is a chapter one about introduction. Then there is chapter two, here literature review is presented and various models are analyzed critically then a theoretical research model is developed. Chapter three deals with Analysis and design, here we take a look at the requirement analysis of mobile application. After analysis of requirements we move to the design of the product. Chapter four looks at the implementation of the prototype. The actual coding will be attached as an appendix, so only the implementation framework is discussed. Next we look at the most important component of the research which is the security analysis and usability analysis of mobile solutions in respect to the proposed model. In chapter five we look at the general discussion, the recommendation and conclusion.

1.3 Problem Description

Utility providers face a major task in collecting monthly data from their investments which can be countrywide or within a city or a town. This monthly data is the source of their core income. Therefore any inefficiency results in serious financial problems which can lead to poor services and eventual collapse. For example the city council of Nairobi failed in water meter reading leading to outsourcing to an independent Nairobi City Water & Sewerage Company LTD (NWC) which by the look of things is headed for failure if they don't reengineer the way they read their meters and update their systems promptly and accurately as well as linking it to customer care for prompt customer information. There is need to utilize technology in the most cost effective way while minimizing the workforce involved in order to increase the return on investment. Faced with these facts and given that mobile networks now covers most parts of the country, mobile technology can be used to enhance service efficiency while minimizing the cost of operation.

1.4 Project Justification/Motivation

The inefficiency shown by the utility providers in carrying out their core business is perplexing to say the least. The Nairobi water company for example has completely failed to read their meters monthly and have resorted to inaccurate approximation of customers bills. Each time a customer request for their bills they are given an estimated bill which can be under or over depending on unknown probabilities. When they finally read after 3 to 4 months and updated in the system 1 month later the customer is served with a bill he or she has no idea where it came from or had totally not budgeted for. With this scenario the ever skyrocketing unpaid bills is largely caused by the providers' inefficiency and inaccuracy rather than the customer themselves.

Talking to management of these providers of why they are not efficient in this current age of technology, they will gladly inform you that the budget needed to computerize these operations especially meter reading remotely and networking their remote offices and branches to their information centre runs into billions of shillings hence they will never afford it. There only hope is that a donor will one day come to their rescue or they will just continue with there survival techniques.

What the management is not aware of is that the simple gadget they have in the name of a mobile device they are so much accustomed to using for communication is the key to streamlining there services. It will actually be cost effective to implement this service which will utilize the existing GSM network of the mobile operators. It will also eliminate the data entry clerks, save on stationery, reduce inquiry and customer service staff and above all ensure that there systems are updated immediately the meter reading is read at the source. The system will also have an SMS gateway such that customers can inquire their balance via their mobile phones. It will also have emailing capability such that immediately the meter is read the system generates dynamically a PDF statement and emails it to the customer.

The beauty of the proposed model is that instead of management thinking where it will get millions of shillings to digitize its operations it will actually save them millions of shillings. Hence the motivating factor is how the mobile devices can actually be used to give these providers a lifeline at a minimum cost where the return is high while meeting the following core factors;

- Cost effective – (time, Monetary and Efficiency)
- Adaptability - device independent.

- Secure
- Portability
- Extensibility

1.5 Research Questions

- What are the types of models that can be used to implement mobile data collection system for utility providers?
- Which model or models are the most cost effective, usable and secure for implementing mobile metering services for utility providers?
- Is it possible to implement a mobile data collection system using the model(s) chosen that is adaptable to the device or browser being used?
- Is the model developed usable by the intended users?

1.6 Objectives

The general objective of this research project is to develop a cost effective secure mobile data collection and customer information model for utility providers and implement it as a system prototype to show how utility providers can utilize the system using WAP enabled mobile phones to enable updating of the central system from the remote location of the meter and link this to customer care service automatically. We also look at security, vulnerability and user analysis of the model.

Specific Objectives

- To carry out analysis of existing data collection models.
- To identify ways in which data capture, analysis and customer care workflow can be reorganized and made more efficient.
- To analyze security and vulnerability of the prototype and what enhancements can be done to make it more secure.
- To identify cost effective ways in which hand-held devices can be used for data collection.
- To develop a working prototype of the system based on the proposed model
- To carry out usability analysis of the prototype.

1.7 Project Scope

An important part of this research project will be to develop a data collection model and implement has a prototype system. Functionality is the main focus of the prototype system. The prototype will have all the functionality required to successfully perform a laboratory usability test. Since the security of the solution is transparent for the users, this will be partly implemented to save on time and resources required e.g. the RADIUS server. A preliminary security and usability analysis will be conducted. Suggestions on what security measures should be implemented in the system will be made based on the results from this analysis. The suggestions will focus mainly on measures for securing the wireless link, authenticating the devices and protecting the data. Detailed security analysis is beyond the scope of this project, because it would require specific security measures to be implemented. Usability analysis will be done using participants from real intended users. This involves letting participants test the prototype then answer the usability questionnaire based on the test in order to analyze the usability of the proposed model.

CHAPTER 2: LITERATURE REVIEW

2.1 Background Information

Utility providers are companies or organization or government departments that provide metered services to the public. Currently we have two main utility providers the water services which are mainly controlled by the local government with each local council being entitled to manage water services within there area of jurisdiction. The second provider is Electricity providers which is mainly controlled and managed by the Kenya power and lighting company (KPLC) with government having majority shares. Both these providers face the same problem of trying to automate there meter readings and none has so far made any headway. Although KPLC are in the process of installing digital meters the remote meter can directly communicate with the base station for eventual updating of the systems. However this is still a pipe dream and requires huge investment to install. For the Water services, there problems are still so basic that they actually need something if they are to even start thinking of changing current meters to digital.

2.2 Mobile data collection models

2.2.1 The World Wide Web model

The WWW model, or simply the web, used on the Internet gives a client the possibility to receive contents in a well-specified data format from web servers. The communication is handled through standard networking protocols such as HTTP and TCP/IP. To reach the content on the server the client uses addresses in a standard naming model called Uniform Resource Locator (URL) as shown in Figure 1.1 The client uses a Web Browser to view the content provided and among the formats supported are a language to describe the appearance of the content called HyperText Mark-up Language (HTML) and a script language to enhance the content functionality called JavaScript or vbScript. It is a stable model that has been used to develop the WAP model [7].

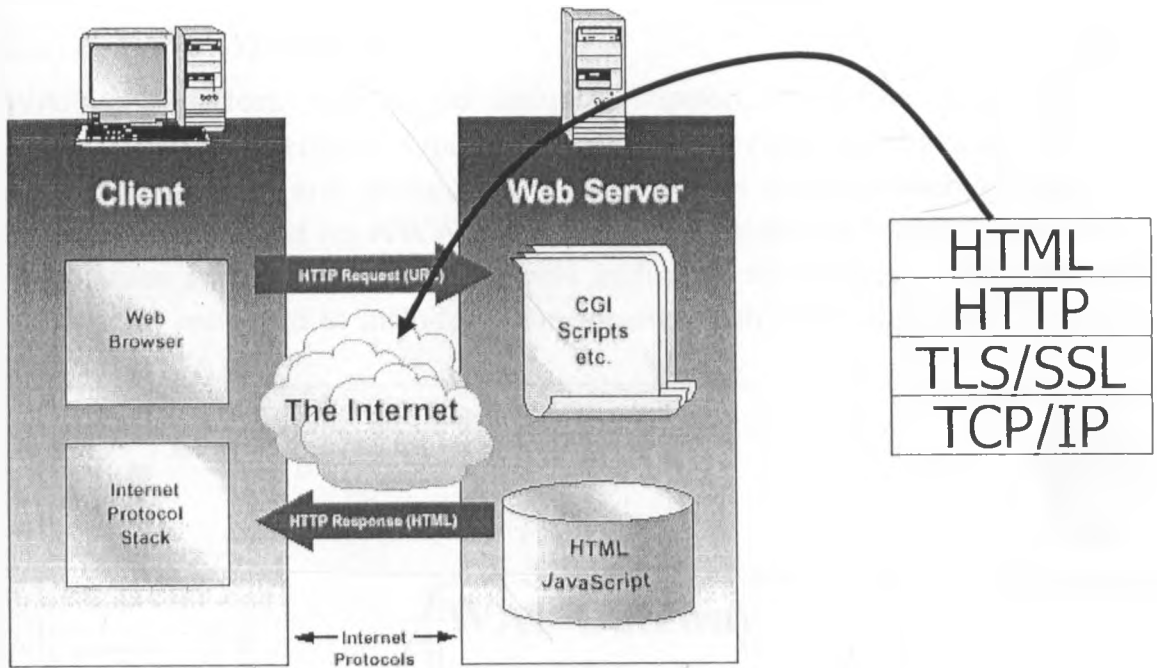


Fig 1.1: WWW Model (source WAP forum)

Advantages of WWW Model

- It's a stable accepted standard model within the field of computing
- High number of experts to develop application for this model are available
- Supports exchange of high volume of information unlike the WAP model.
- Highly secure using SSL (Secure HTTP)
- Can utilize any existing public and private network

Shortcomings for WWW Model for mobile applications

- It is designed for large bandwidth, low delay
- Its stateless, client/server, request/response communication
- Its based on connection oriented, one connection per request
- High overheads TCP 3-way handshake, DNS lookup overheads
- Has big protocol headers, uncompressed content transfer
- primitive caching (often disabled, dynamic objects)
- security problems (using SSL/TLS with proxies)
- designed for computers with "high" performance, color high-resolution display, mouse, hard disk
- typically, web pages optimized for design, not for communication; ignore end-system characteristics

2.2.2 WAP MODEL

WAP is an effort, with broad industry support, to define a standard for communicating Internet – type information to devices that have roughly the same form factor and processing power as the average mobile telephone. WAP model is based on WWW model which has stable architecture and ability to embrace and enhance existing tools including web-servers, XML tools etc. It has been enhanced to include Enhancements Push technology and Telephony Support (WTA) [7].

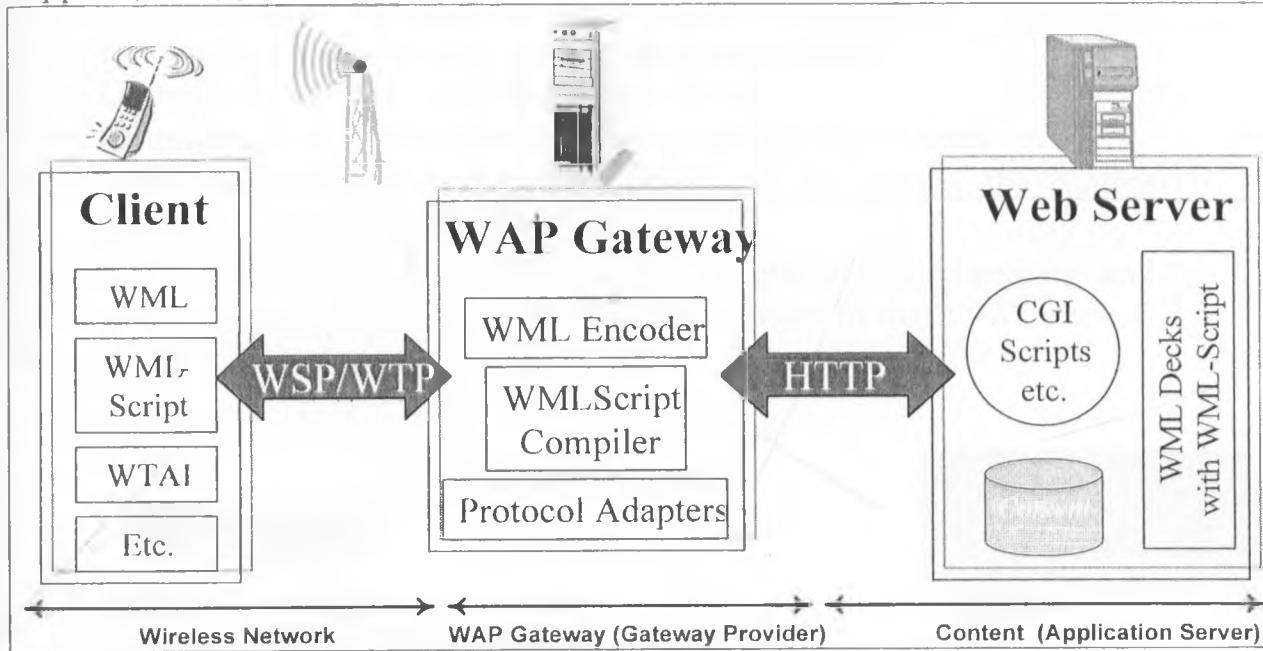


Fig 1.2 WAP (source WAP forum)

The diagram below shows the conversion of a wml page from a Webserver to the mobile device.



WAP is designed for

- Primarily includes mobile phones, pagers and PDAs
- Low bandwidth and high latency environments
- Unpredictable stability and availability
- Limited processing power and battery life
- Less memory (ROM and RAM)
- Smaller displays

WAP Objectives

- Create global wireless protocol specifications that work across differing wireless technologies
- Facilitate network-operator and third party service provisioning
- Define a layered, scalable and extensible architecture
- Bring Internet/Intranet information and advanced data services to wireless terminals
- Optimize for efficient use of device resources
- Provide support for secure applications and communication
- Embrace and extend existing standards where possible
- Optimize for efficient use of device resources
- Optimize for narrowband bearers with potentially high latency
- Enable personalization and customization of the device, the content delivered to it and presentation of the content

In order to ensure that the WAP inherits the stable tested security and functionality features of WWW its layering (stack) maps to the WWW stack as shown below

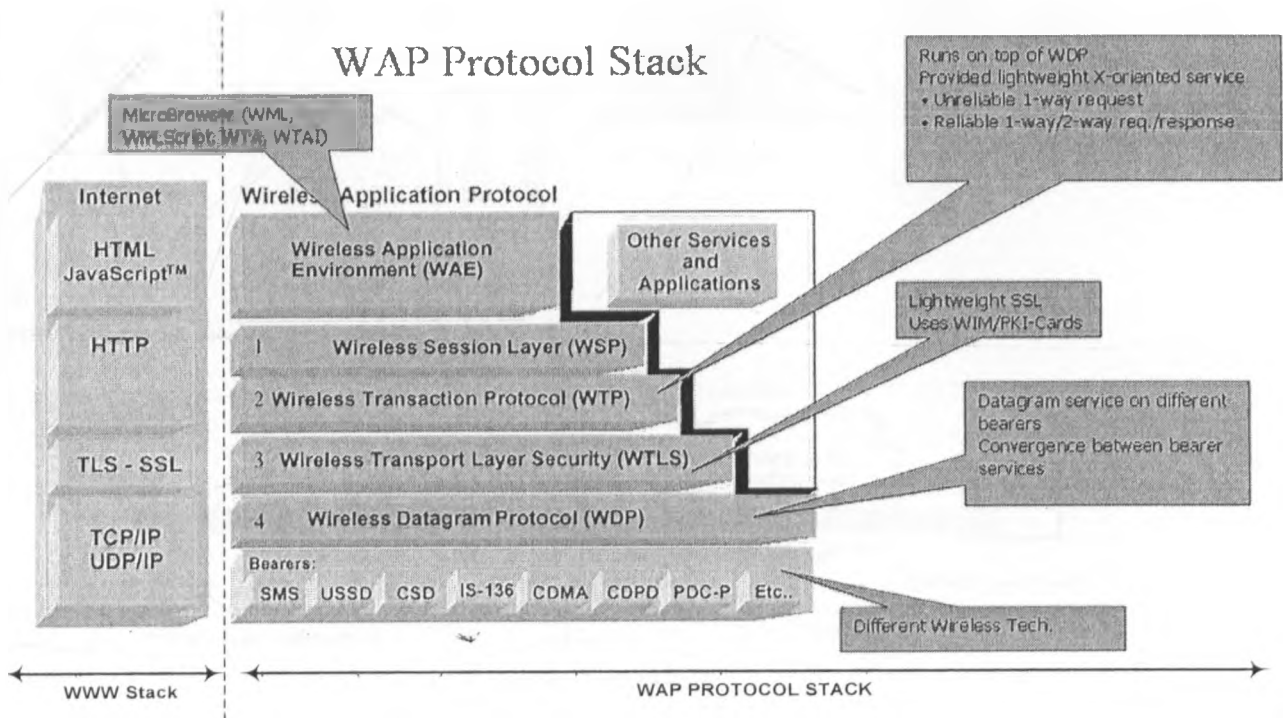


Fig 1.3 WAP Protocol Stack (source WAP forum)

WAP Model Security

Since WAP is using existing technologies as much as possible there is a lot of communication over the World Wide Web domain and not just only over the wireless community. This leads to the need of two different security protocols, SSL for the web and WTLS for the wireless part. The WAP gateway becomes the link between those two parts as shown in Figure 1.4. Since all traffic must be decoded and re-encoded in the gateway there are some strict rules for the gateway to follow. First of all it is not allowed to store any decrypted information on secondary media. The whole conversion process has to occur in volatile memory and all information must be deleted as soon as the conversion is finished. The only access to the gateway that can be allowed is authenticated logins by an administrator within the gateway's domain. This is to ensure the users and service providers that the information will still be secure and not fall into any other party's hands despite the conversion process.

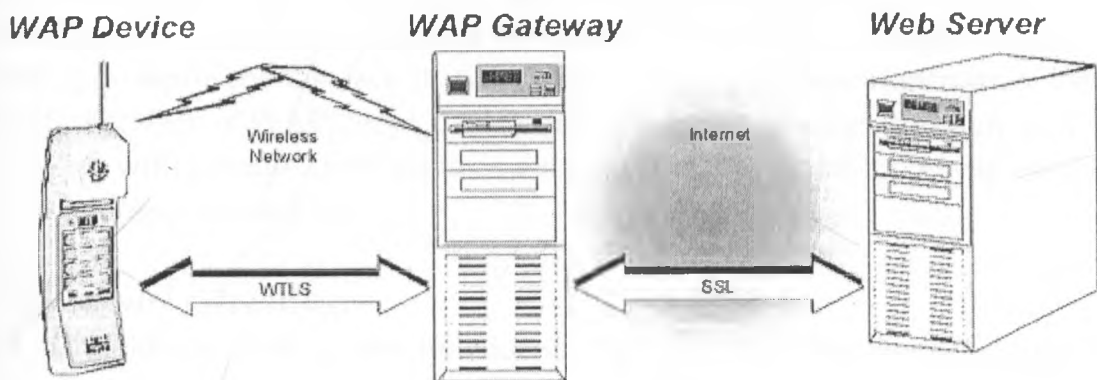


Fig 1.4 WAP Model Security Analysis
Security Loop holes of the WAP Model

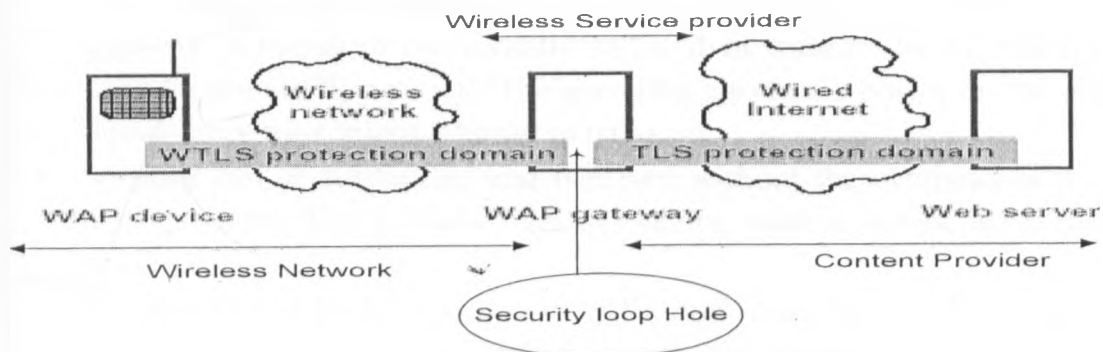


Fig 1.5 WAP Security Loop Hole (source Yasir Zahur Independent Study)

Considering that wireless networks are generally more vulnerable than wired networks, a number of wireless security standards have been developed to ensure the security of information transmitted over the wireless Internet. For instance, Wireless Application Protocol (WAP) solutions use the wireless transport layer security (WTLS) in place of Secure Socket Layer (SSL) or Transport Layer Security (TLS) to ensure secure transmissions between WAP client devices and the WAP gateway. However, communication between the WAP gateway and the backend application or Web server is over a wired network and thus uses standard TCP/IP based Internet security protocol such as TLS or SSL. This scenario therefore creates a need for inter-protocol translation to be handled within the WAP gateway. This results in what is known as the “**WAP gap**” (Security loop Hole), which is a subtle security issue within WAP-based solutions. The WAP gap occurs due to the inter-protocol translation or conversion process, which causes encrypted data to be decrypted, albeit momentarily, and then re-encrypted before transmission from the WAP gateway to either the WAP client device or the backend application or Web server. The WAP gap represent the fact that every encrypted message transmitted using WTLS, between a WAP client device and the wired Internet through a WAP gateway, will at some brief instance exist as readable plaintext whose security could be compromised [18].

WAP model advantages

The list below is some of the functionalities that reduce the workload and the power consumption for the client. It will give the user more operating time as well as a cheaper device, since it does not need as much computing power.

- All information, including the HTTP headers, is binary encoded by the WAP gateway. The amount of data to deliver between the client and the gateway is therefore significantly reduced in contrast to the plain text used by the HTTP protocol. The encoding also saves power on the client device since the content is easier to parse.
- Sessions can be suspended and resumed without the overhead of initial establishment. This is useful, besides saving power, to free up network resources.
- The number of packages needed by the transaction protocol is reduced, since there is only one route between the gateway and the client. Therefore the need to manage unordered packages does not exist.
- The gateway handles all the DNS services to resolve domain names used in the URLs. This means that no extra packages for name translation have

to be sent over the wireless domain. However, this is not a unique advantage of WAP since it can be achieved with a HTTP proxy as well.

- From version 1.2 of the WAP protocol push functionality will be available. This means that a content provider can push information to the user whenever it is appropriate, e.g. to inform the user of changes or events.
- The improvements made to the protocol stack lead to significant savings in bandwidth. Here is a query from a HTTP 1.0 compatible browser compared to a query from a WAP browser. With a typical handset session with three requests and three responses less than half the number of packages is needed by the WAP protocol stack, which leads to the fact that while the HTTP 1.0 stack have 65% overhead the WAP stack only needs 14% overhead [18].

WAP Model disadvantages

- It is very difficult to configure WAP phones for new WAP services, with 20 or so different parameters needing to be entered to gain access to a WAP service.
- There are few mobile phones that support WAP and widespread WAP support in handsets is unlikely for a long time. The problem is also compounded by change in technology frequently. Since the solution targets on mostly the meter readers it wont be a big hindrance to the proposed model
- There are many WAP Gateway vendors out there competing against each other with largely the same standardized product. This has led to consolidation
- The WAP gap security loop hole. Lack of end to end security due to change of protocol between the WAP gateway and the WWW model

2.2.3 SMS Model

The initial idea for SMS usage was intended for the subscribers to send non-sensitive messages across the open GSM network. Mutual authentication, text encryption, end-to-end security, non-repudiation were omitted during the design of GSM architecture [20].

Security Deficiencies of GSM Architecture

Much as GSM system strives to make a provision for security services it still has limitations in its security. Tasneem et al (1998), point out the lack of data integrity in the GSM. On top of this the following cryptographic issues with regard to the authentication and encryption algorithms have been identified.

- *Problems with the A3/A8 authentication algorithm-* A3/A8 is the term used to describe the mechanism used to authenticate a handset on a mobile phone network. A3 and A8 are not actually encryption algorithms, but placeholders. In A3/ A8 the commonly used algorithm is COMP128. COMP128 was broken by Wagner and Goldberg in less than a day. This raises concerns of having GSM as a secure communication mechanism. After cracking COMP128 Wagner and Goldberg went on to prove that it was possible to obtain the Ki value, therefore making it possible to perform SIM cloning.
- *Problem with A5 Encryption Algorithm-* The A5 algorithm is used to prevent casual eavesdropping by encrypting communications between mobile station (handset) and BSS. Kc is the Ki and RAND value fed into the A5 algorithm. This Kc value is the secret key used with the A5 algorithm for encryption between the mobile station and BSS. There are at least three flavours of the A5 algorithm. These include A5/1 which is commonly used in western countries. The A5/1 is “deemed ‘strong’ encryption” but it was reverse engineered some time ago. A5/2 has been cracked by Wagner and Goldberg, the methodology they used required five clock cycles making A5/2 almost useless. Finally A5/0 is a form of A5 that does not encrypt data at all. All these problems with the A5 encryption algorithms prove that eavesdropping between mobile station and BSS is still possible, making SMS and GPRS over the GSM core network very insecure for secure mobile *Solutions*.
- *Attack on the RAND value-*When the AUC attempts to authenticate a SIM card, the RAND value sent to the SIM card can be modified by an intruder failing the authentication. This may cause a denial of service attack. [20]

Having described the communication medium used by SMS we now look at the SMS model. The SMS model is composed of the mobile phone, the GSM network, the mobile network provider and the Client as shown in figure 1.6 below

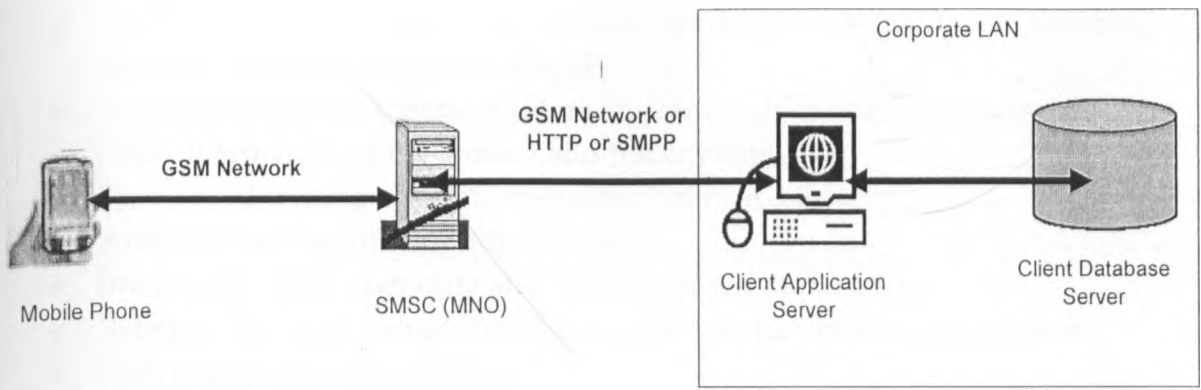


Figure 1.6 SMS Model

Security Problems with SMS

The initial idea for SMS usage was intended for the subscribers to send non-sensitive messages across the open GSM network. Mutual authentication, text encryption, end-to-end security, non-repudiation were omitted during the design of GSM architecture. Below is some of the security problems associated with the SMS model.

- *Forging Originator's Address* -SMS spoofing is an attack that involves a third party sending out SMS messages that appear to be from a legit sender. It is possible to alter the originator's address field in the SMS header to another alpha-numerical string. It hides the original sender's address and the sender can send out hoax messages and performs masquerading attacks. This is common among messages originating from web interfaces using the WWW model.
- *SMS Encryption*-The default data format for SMS messages is in plaintext. The only encryption involved during transmission is the encryption between the base transceiver station and the mobile station. End-to-end encryption is currently not available. The encryption algorithm used is A5 which is proven to be vulnerable. Therefore a more secure algorithm is needed.
- *Denial of Service Attack*-There is security vulnerability at the SMS Centre (SMSC). When an SMS message is received at the SMSC, the message gets queued up at the storage buffer. The attacker can exploit this vulnerability by flooding the buffer queue with multiple meaningless messages to a target mobile number. This type of flooding can causes the SMSC to reject incoming messages for the victim because the storage space is limited in the buffer queue [19]

advantages

- Enables wireless data access for corporate users.

- Notification mechanisms for newer services such as those utilizing wireless application protocol (WAP)
- Protection of important network resources (such as voice channels), due to SMS' sparing use of the control and traffic channels
- Delivery of messages to multiple subscribers at a time
- Ability to receive diverse information
- Integration with other data and Internet-based applications
- Reliable, low-cost communication mechanism for concise information
- Guaranteed message delivery
- Delivery of notifications and alerts

Disadvantages

- Insecure mode of data transmission
 - A5 encryption algorithm is not entirely secure. Research has shown that this method has flaws and it is vulnerable to attacks.
 - If the message content is not encrypted then any personnel who have access to the service provider's SMS data can view the sensitive details.
 - The verification depends only on the sender's number, such that if the SIM card is lost or the SIM card is duplicated, the attacker can use the victim's account to perform transaction.
 - The SMS message that gets sent to the application server is only encrypted between the mobile station and the base transceiver station. The message is in plaintext within the mobile operator's network.
 - By allowing customers to send their authentication PIN, the service provider can read the PIN because it is sent in plaintext.
- Lack of interactivity to real time data sources
- Length limit of 160 characters
- Expensive mode of data transfer compared to the WAP model and WWW model
- Unable to control input format

2.2.4 Secure SMS Model

The confidentiality of the message content transferred from the mobile phone to the application server must be preserved. Any unauthorized individual who managed to obtain the message must not be able to read the secured contents within the SMS message. Only the parties with the correct security details can acquire the message content. If the transmitting message was altered, the receiver should be able to notice the message content is changed.

The structure of the secure SMS application system is broken down into a three tiers system. The mobile application is responsible for generating the secure SMS message and sends the message via SMS across the GSM network to the destination server. The Application server has listeners that constantly listen for incoming messages and the server application decodes the received messages into a program interpretable format. The application server follows the designed secure SMS protocol to verify the security of the received message. The backend database contains all the application details and security details of the users. Figure 1.7 illustrates a graphical representation of the Secure.

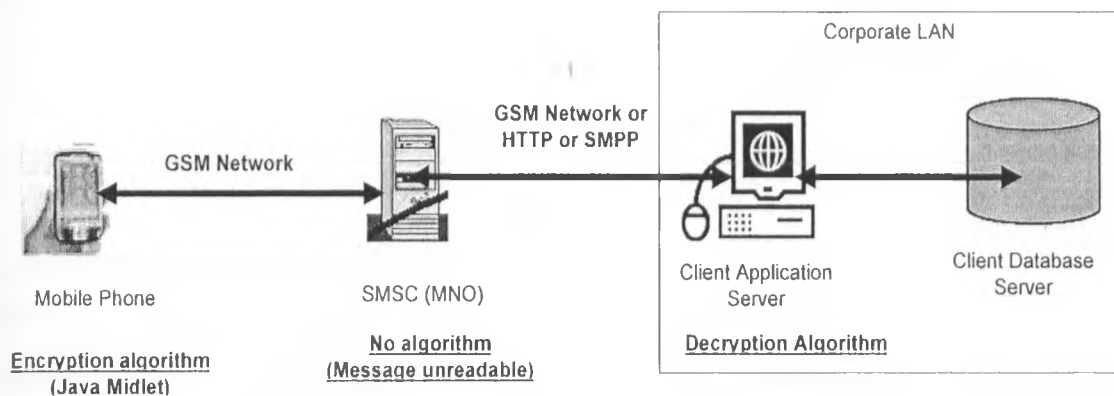


Fig 1.7 Secure SMS Model

Mobile Application Component-This MIDlet application runs on the client mobile device and is used to access and send message. This ensures that authentication and encryption and decryption of message is done only by the application

Application Server-It is responsible for receiving and decoding the secure SMS message. The server will check to ascertain that the message is suitable for a secure SMS protocol. It will then proceed to check for the account identifier from the message and find out if the identifier exists in the server database. After the above check the server decrypts the message using the one time password. The password will be discarded when the decryption is successful.

Database Server-Stores the main database of the organization, it is linked to the Application server.

Secure SMS Protocol Layers

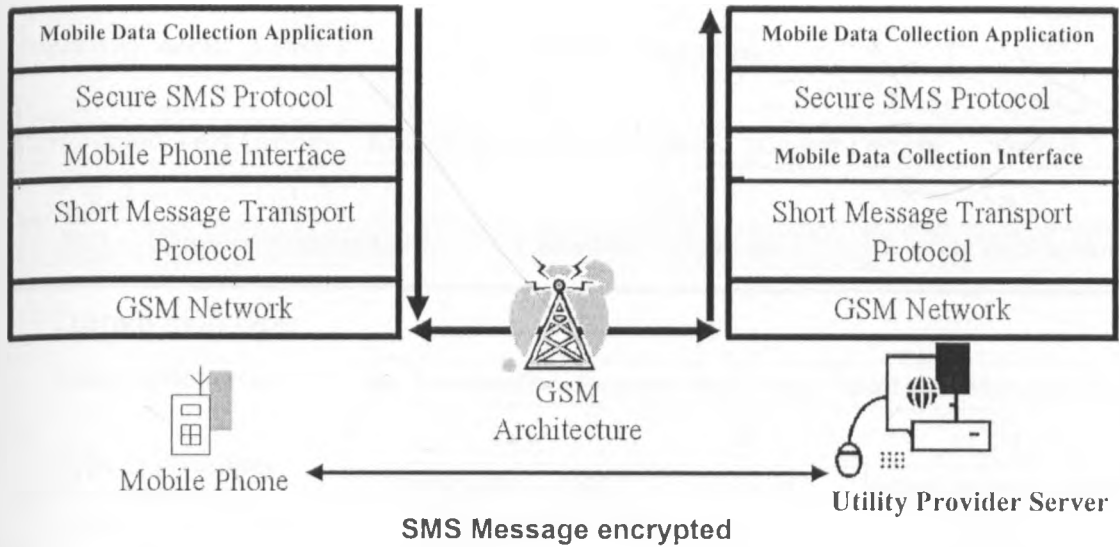


Fig 1.7 Secure SMS Protocol Stack

Secure SMS Protocol Message Structure

The secured SMS message is divided into multiple fields to accommodate for the various security checks required for the protocol. To ease the understanding of the message structure, Figure 1.8 shows the structure overview for a secure SMS message. The numbers above the fields are the minimum number of bytes required for each field in the message. The number of bytes for each field can be increased depending on the implementation requirements.

The use of each labeled structure is explained below:

- The *Version* is the mobile application version number. It contains a specified bytes pattern. The receiver checks if the first three bytes of the received SMS message are valid for the application server. If the message version number does not match the application version, then the message is discarded. As there are possibilities that the server can receive accidental SMS messages that are not intended for the application server. The usage of the version bytes is to help to eliminate these erroneous messages.

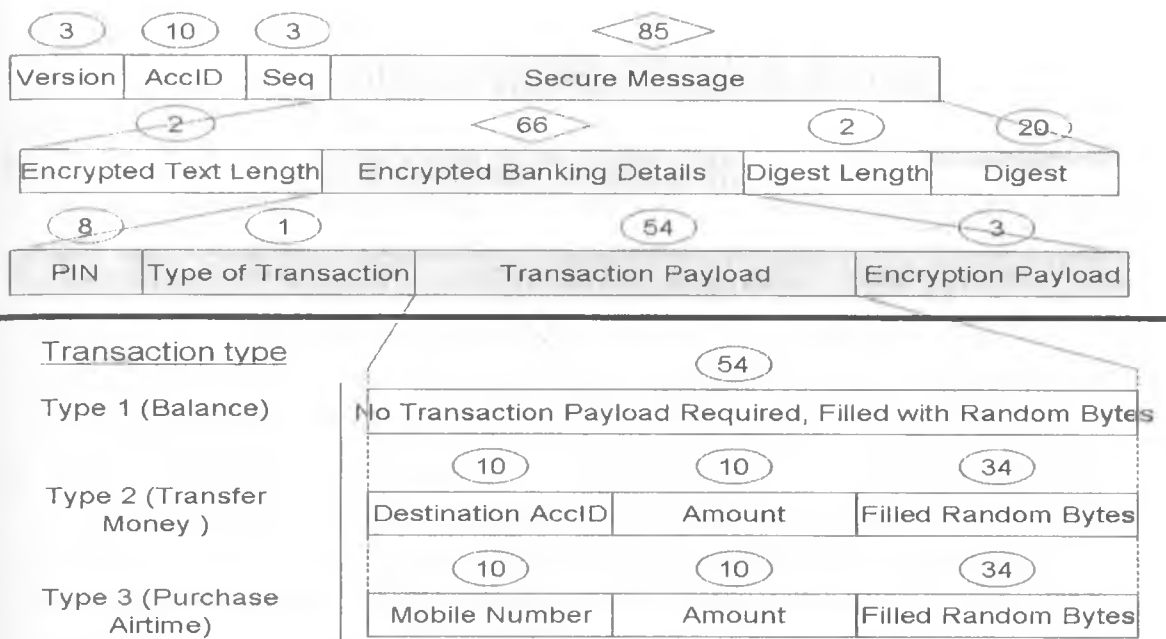


Figure 1.8 The Structure of a Secure SMS Message

- The *AccID* contains the customer account identifier of the user.
- The *Seq* is the user's current sequence number of the one-time password.
- The *Encrypted Text Length* contains the number of next bytes that are the ciphered message.
- The *Digest Length* contains the number of next bytes that contains the message digest.
- The *Digest* contains the calculated digest value of the message. The use of the digest is for the server to check for message integrity. For the secure SMS protocol, a single digest of the following fields is calculated: *Version, AccID, Seq, PIN, Type of Transaction and Transaction Payload*.

The content of the following fields is encrypted using the generated session key.

- The *PIN* contains the user predefined password. This is used by the receiver application to authenticate the user.
- The secure SMS message can be used for different types of transactions. The *Type of Transaction* is used by the application server to identify the type of transaction it should perform.

The *Transaction Payload* is the extra data that is used for a transaction, but it is not used for any security purpose. The content of the *Transaction Payload* depends on the type of transaction requested. The structure of the payload depends on the type of transaction offered by the Client [20].

Advantages of secure SMS model

Apart from inheriting all the advantages of SMS model the secure SMS model has the following security advantages.

- *Confidentiality*-This is achieved by encrypting the message using a symmetric secret one-time password. The one-time password is only shared between the user and the application server. The strength of the confidentiality depends on the security strength of the passwords generation algorithm used and the strength of the ciphering algorithm used. It is assumed that only the authorized user will know his/her list of passwords and the passwords are never shared with other people.
- *Integrity*-The message digest is the hashed value of the message content calculated server application and the mobile phone application. If the content is altered during transmission, the hashing algorithm will generate a different digest value at the receiver side. If the digests mismatch, the receiver will know that the integrity of the message has been compromised. The strength of the integrity checks depends on the strength of the algorithm used to generate the digest value and it also depends on the strength of the encryption algorithm used to hide the confidential data.
- *Authentication*-For the receiver to authenticate the user, the user must provide his/her authentication detail(s) to the receiver. This authentication process is performed by validating the message PIN with the receiver stored PIN. The PIN is previously selected by the user when the user registers for a mobile application account. The strength of the authentication depends on the password selection strategies used.
- *Non-Repudiation*-Only the account holder and the application server are supposed to have the one-time password. The application server does not generate the same one-time password more than once. Therefore every one-time password is unique in the server's database. Each pair of one-time password and sequence number is only allowed to be used for a single user. Therefore the user cannot deny not sending the message because only that specific user has that unique pair of password and sequence number to encrypt the message. If the application server can use the same sequence-password pair to decrypt the message, then it indicates that user must have sent the message.
- *Availability*-The availability of this protocol depends on the availability of the cellular network. The time it takes for a message to be delivered depends on the density of network operator base towers. The number of transactions that the server can handle at once depends on the hardware capability. If the server's hardware can handle multiple incoming messages then the server can perform multiprocessing to accommodate for more requests. The protocol

has no restriction on the type of hardware needed. Therefore it is up to the developers to decide the hardware specifications. Apart from the security issues being addressed the format of the input is also controlled because the user interface is controlled by the MIDlet application developed.

Shortcomings of this Model

For this model to work in a large organization it requires an SMS gateway which is mostly provided by a third party companies licensed by CCK unless the company acquires their own SMS Gateway. It is also affected by the shortcomings of the SMS which can only allow upto 160 characters hence not viable for a fully fledged system. Unlike the WAP model which utilizes the traditional web interface systems, the client mobile devices have to be installed with the mobile application component hence costly to maintain and support. Also the model has the following thread offs

- Cost – charges per SMS not per the size of transfer
- Language specific - J2ME
- Security vs. Performance trade-off
- Security vs. Functionality trade-off
- Hardware Platform (Compatibility)-MIDP 2.0 Compliant. Not all mobile devices support this platform
- Limitation of SMS Length (160 characters)
- Problems associated with Client server technology for example need to update handsets every time modification is done.
- Need to learn new platform of development. That's does not utilise the existing stable programming paradigm of WWW model.
- Not easy to extend and increase functionality.
- Does not support high level of interactivity.
- Having the application loaded onto the SIM card makes the mobile application SIM card dependent. If the SIM card is lost, the security of the mobile application is vulnerable.
- Unlike the WWW model and WAP model it is based on SMS processing hence concurrency processing and scalability might be hard to achieve.

2.3 Existing Mobile Data Collection Systems

The solutions provided are numerous and varied but we will highlight just a few of them related to the models we have described above:

Automatic meter reading (AMR) Systems - Using wireless radio transmitters, AMR remotely reads customer meters and then transfers the data

into the billing system. AMR will reduce the need for meter readers to manually gather utility meter readings each month. Many utilities are using AMR as a way to improve customer service and control their meter reading costs, especially in areas with fenced yards, dogs, landscaping and other issues that make accessing meters difficult or unsafe. The modules transmit meter readings and the meter identification number. Diagnostic information is also transmitted to verify that the meter is operating correctly or notify us of a power outage. Below is a diagram showing how the system works:

This wireless automatic system is based on *WWW Model* intranet version or the client server architecture. The wireless connection is owned and controlled by the utility provider. The meter acts has the client machine posting data to the billing system.

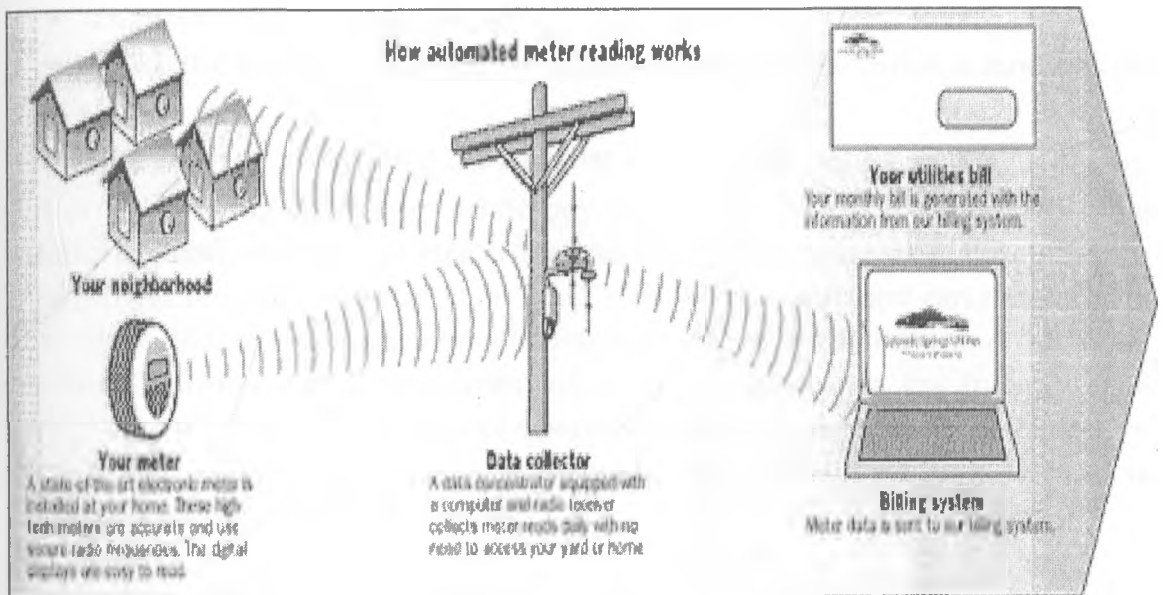


Fig 1.9: AMR Solution

Advantages

- Improved customer service.
- Minimizing the need to access your property to read your meters.
- Call resolution improvement – billing calls will be handled more quickly due to availability of more frequent meter readings.
- You won't need to read your own meters if we can't access it.
- Controlled meter reading costs.
- Fewer employee injuries, especially in areas with fenced yards, dogs and landscaping.

- A reduction in operational costs that will save you money.

Why it's not a preferred Solution to this project

The goal of this project is to minimize implementation cost as much as possible. This option is not viable for the NWC since:-

- They have to replace all there water meters which are already in use.
- They will have to install or give a third party AMR and the cost associated with this solution is prohibitive. Average of \$2000 dollars per digital meter
- Need to hire new skilled expatriates or train existing staff to manage the solution
- Need to change there existing solution since AMR is not an open source solution rather than a package provided by specific companies.
- It takes a very long period to implement usually more than 5 years in developed countries.
- Maintenance of electronic meters more frequent than current existing meters.
- Industrial relationship issues.
- Since the system is not open, it's not easy to build additional modules on top.

Remote Meter Reading Solution - The remote meter reading software and accompanying hardware technology is state of the art. It allows real time monitoring and metering of electricity, gas and water using existing electricity lines (power line communication or "PLC"). The utility company can receive data from individual homes or apartment complexes on an hourly basis and can allow the same information to be distributed to its customers via the internet. The result is significant as it will reduce operating and administrative costs, improve energy management and pricing structures and customize billing. Below is diagram of its implementation:

UAS System Technical Schematic

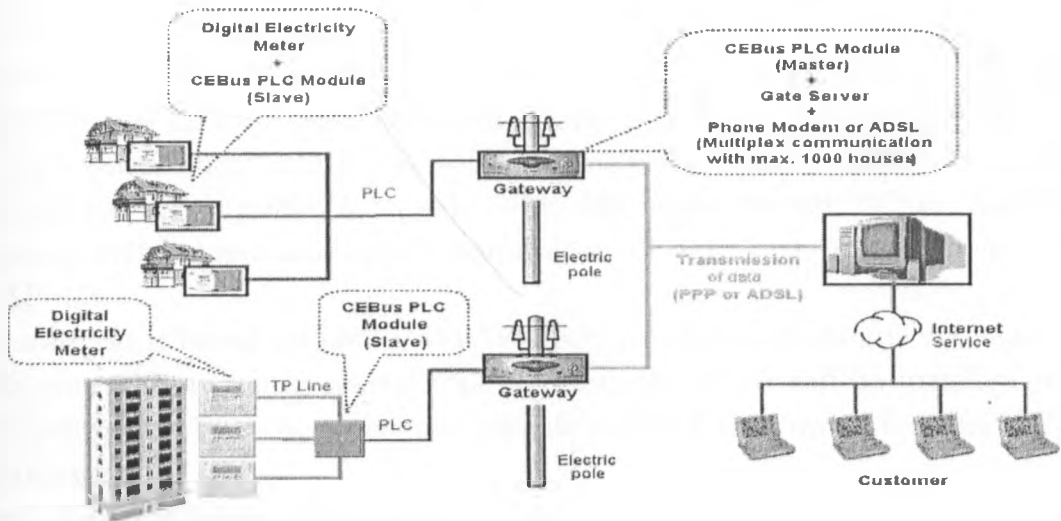


Fig 2.0: UAS System Technical schematic diagram

This wired automatic system is based on WWW Model. The meter acts as the client machine posting data to the billing system [12].

Advantages

- Use already existing lines of communication
- High reliability
- Various applications
- Easy monitoring and management
- Customer accessible management program through internet

Why it's not a preferred Solution to this project

- They have to replace all their water meters which are already in use with digital meters and connect to electricity line.
- Assumes each homestead has a telephone or electricity line for communication
- Expensive to install and maintain
- Need to hire new skilled expatriates or train existing staff to manage this solution
- Need to change their existing solution since this solution is not an open source solution rather than a package provided by specific companies.
- It takes a very long period to implement usually more than 5 years in developed countries.
- Does not utilize the emerging technology of mobile communication.
- Maintenance of electronic meters more frequent than current existing meters.

Celesta Meter reading solution - With this wireless meter reading solution meter readers will use their rugged PDA terminals to receive their metering schedules, record the metering data on site and send the readings wirelessly over GPRS to SAP back-office system. Process integration is based on Celesta's proprietary mBusiness software platform, which enables intelligent applications on portable terminals with Microsoft Pocket PC or Symbian operating systems and push/pull communications with back-office systems such as SAP R/3.

This solution is based on secure *WWW Model* where application is accessed via GPRS connectivity using special mobile terminals which can be installed with Microsoft pocket PC hence system accessible via internet browser for pocket PC.

Advantages

- High reliability
- Easy monitoring and management
- Customer accessible management program through internet
- Uses wireless technology

Disadvantages

- The system is very costly to implement since it's closed and installed and maintained by the supplier.
- Leads to over reliance on the supplier
- Expensive to install and maintain
- Need to hire new skilled expatriates or train existing staff to manage this solution
- Need to change there existing solution since this solution is not an open source solution rather than a package provided by specific companies.
- Forces companies to purchase SAP solutions which is very expensive.
- No local support.
- Does not support variety of mobile devices

Customer SMS - This is a two way Short Message service (SMS).

Where the Customer reads the reading and sends a text message via a third party SMS Gateway to companies system for updating of his record.

This model is based on the SMS model. But instead of using the meter reader, the company accepts SMS from customers and bills them.

Advantages

- Cheaper to implement.
- Consumes less bandwidth.
- Time efficient

- No need of Meter Readers

Why it's not a preferred Solution to this project

- This solution is very insecure because SMS are meant to send very basic none critical information via the network.
- Data can easily be accessed by unauthorized personnel
- Need to send data in a given format hence prone to errors
- Reliance on a third party who enhance introduces a point of inefficiency.
- Expensive to maintain monthly third party charges.
- Need to verify entries before batching them to the central system
- It depends mostly on the honesty of the customer

2.4 Enabling Technologies

Here we describe various mobile network technologies, where some are currently in existence on global mobile networks, while the other technologies are gradually becoming adopted by mobile operators. A technical description is outlined for some of the communication services for these network technologies.

Mobile Network Technologies

- **GSM** - Global System for Mobile Communication is a second generation standard for mobile Communication, developed by the European Telecommunications Standards Institute (ETSI) and now currently owned by the Third Generation Partnership Project (3GPP). Operating in the 900 MHz and the 1800 MHz frequency band, GSM is the most widespread mobile standard currently in use across Europe and the Asia-Pacific region [24].
- **GPRS**- General Packet Radio Service is packet switched wireless protocol providing non voice value added services that allows information to be sent and received across a mobile telephone network. It is described as a 2.5G technology which supplements Circuit Switched technology such as GSM. Data transmissions speeds of 9.6 kbps to a theoretical maximum speed of up to 171.2 kbps are achievable with GPRS using all eight timeslots at the same time. In addition to higher data rates, GPRS provides users with all time connectivity while only charged for the data viewed or received with a minimal online charge [24].
- **EDGE**- Enhanced Data for Global Evolution is a higher bandwidth version of GPRS permitting transmission speeds of up to 384 Kbps. It is compatible with the GSM protocol, but it requires higher quality radio signals to reach the increased speed[24].

- **3G** -3rd Generation is the generic term for the next big step in mobile technology development. The formal standard for 3G is the IMT-2000 (International Mobile Telecommunications 2000). There are three optional modes as part of the 3G standard. W-CDMA (Wireless Code Division Multiple Access) is for Europe and for the Asian GSM countries, CDMA (Code Division Multiple Access) is for North America, and then TDD/CDMA (Time Division Duplex/CDMA) for China [24]..
- **CDMA** - Code Division Multiple Access is a proprietary standard for mobile communication, where GSM is an open standard. CDMA was pioneered by Qualcomm and enhanced by Ericsson. Both standards are in competition for dominance in the cellular world. CDMA is a spread spectrum technology, which means that it spreads the information contained in a particular signal of interest over a much greater bandwidth than the original signal. A CDMA call starts with a standard rate of 9.6 kbps, which is then spread to a transmitted rate of about 1.23 Mbps [24]..

Communication Services

- **SMS** -Short Messaging Service was created as a part of the GSM Phase 1 standard to send and receive short text messages, of 70-160 alphanumeric characters in length, to and from mobile phones MS is a smart service, as it can store messages when the target mobile device is switched off and forwards the messages when the unit is again in use. SMS applications are voicemail/fax notifications, delivery of replacement ring-tones, operator logos and group graphics, unified messaging, personal communication (text messaging), and information services. Basically, any information that fits into a short text message can be delivered by SMS [24]..
- **WAP**- Wireless Application Protocol is a technology which provides a mechanism for displaying internet information on a mobile phone or any wireless device. This is done by translating internet information in to a format which can be displayed within the constraints of a mobile device. To obtain Internet access on a mobile device, the device should be WAP-enabled and the web site information should be described in WML (Wireless Markup Language) format. WML is the mobile equivalent to HTML for web pages.
- **E-mail**- Short for electronic mail and often abbreviated to e-mail, email or simply mail, is a store and forward method of composing, sending, storing, and receiving messages over electronic communication systems. The term "e-mail" (as a noun or verb) applies both to the Internet e-mail system based on the Simple Mail Transfer Protocol (SMTP) and to X.400 systems, and to intranet systems allowing users within one organization

to e-mail each other. Intranets may use the Internet protocols or X.400 protocols for internal e-mail service supporting workgroup collaboration [16].

Implementation Programming Languages

- **XML-** XML (Extensible Markup Language) is a formal recommendation from the World Wide Web Consortium (W3C) for describing and displaying the content. It is a structured set of rules for how one might define any kind of data to be shared on the Web. It is similar to the language of today's Web pages, the Hypertext Markup Language (HTML). Both XML and HTML contain markup symbols to describe the contents of a page or file. HTML, however, describes the content of a Web page (mainly text and graphic images) only in terms of how it is to be displayed and interacted with. XML describes the content in terms of what data is being described [24].
- **VoiceXML** -voiceXML is an application of the XML which, when combined with voice recognition technology, enables interactive access to the Web through the telephone or a voice-driven browser
- **WML and WMLScript-** Content and services in WAP are presented to the phone using the Wireless Markup Language (WML) and the WMLScript programming language. WML is a simple markup language defined with XML and is used to mark the contents of the file as actual text, title, hyperlinks, etc. A WML page is a deck of cards. One card at a time is displayed by the phone. WMLScript is a simple programming language based on ECMAScript and JavaScript, which are usually but not always implemented in WWW browsers. A WAP browser is required to implement WMLScript. WMLScript is used to make WAP pages more dynamic [24].
- **Java and J2ME-** Java is a programming language expressly designed for use in the distributed environment of the Internet. Java can be used to create complete applications that may run on a single computer or be distributed among servers and clients in a network. It can also be used to build a small application module or applet for use as part of a Web page. Applets make it possible for a Web page user to interact with the page. The Java 2 Platform, Micro Edition, Wireless Toolkit 2.0 supports the development of Java applications that run on devices compliant with the MIDP 2.0.

WAP Gateway

There are several gateways in the market that can be used to implement the WAP model. Examples are:

- **Kannel** - Kannel is an open source WAP gateway, which also works as a SMS (Short Message Service) gateway. The Kannel project was founded by Wapit Ltd. in June 1999. Wapit is a member of the WAP Forum. The Kannel gateway is robust and scalable with the capability of successfully handling hundreds of messages per second. Kannel supports the most commonly used SMS centre protocols. Fig below shows the Kannel Model

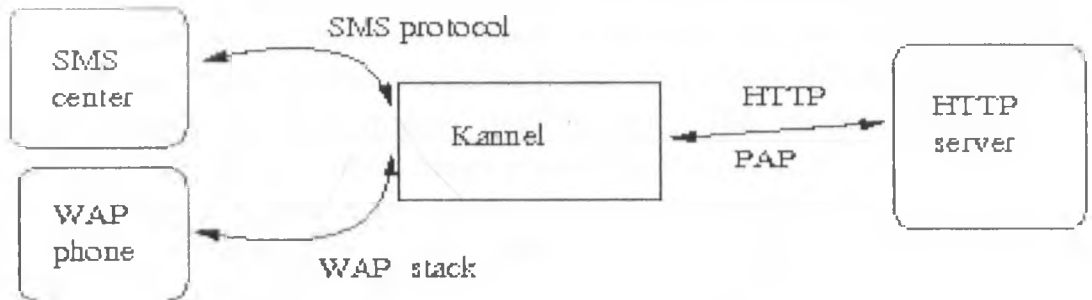


Fig 2.1 Kannel WAP and SMS Gateway architecture (source kannel.org)

The Kannel has been developed using C language and available to the developers as an open source for customization and further development to suite their needs. Kannel is preferred gateway by virtue of being open source it can be customized to suite the needs of the client including enhancement of security by integrating with the RADIUS server and billing Module. Secondly, the advantage of this gateway is that it's 2 in 1 in that it implements both WAP and SMS Gateway. It's highly programmable hence suitable for developers who need to develop very intelligent mobile systems [7].

- **Ophelia**- the Ophelia WAP gateway from 3ui.com enables access of Web-based interactive information, services and applications as well as secure transactions from mobile devices. It is interoperable with a variety of WAP-enabled devices and has built-in support for GPRS and other future mobile technologies. The Ophelia WAP gateway includes the functionality of a protocol gateway as well as content encoders and decoders to translate Web content into compact encoded formats. The modular architecture of the Ophelia WAP gateway enhances system stability in that secure and the non-secure requests can be taken care of by separate servers without duplicating the WAP stack. Thus, each client initiated transaction packet is a message even and thus does not spawn a new

thread. It also has a thread manager which keeps the system from going into an unstable state should there be an overflow of incoming requests [5].

2.5 Theoretical Research Model

In designing the the model to be used as a framework for the development of the mobile data collection and customer information system, we need to first breakdown the functionality components of the system. The model should have the following functionality components:

- *Meter Reading Component* – This component should be mobile, secure, adaptive and have authenticated direct connection to the corporate data source. Update to the system should be online and access should be retracted to authorised users and mobile devices only. The module should be integratable to existing systems hence portability is a necessity.
- *Customer Information Component* – this component is mainly informative hence users or customers don't connect directly to the data source but gets information from the corporate information system based on the information in the system. Here it should support two types of information, the detailed customer billing statement which can only be available via a desktop computers and short informative messages which can be done via SMS. It follows then that billing statement can be done through emailing by sending a PDF billing statement to the customer Email. Short messages can be done via GSM or GPRS.

The model developed should in general meet the following minimum requirements.

- Cost – the model should be cheaper to implement and maintain
- Usability – the model should be usable
- Processing time should be very short i.e. 10 minutes from the time of posting meter reading to the time the customer receives the monthly statement.
- Adaptability – because of change of technology in mobile world there is need for a solution that can adapt to any device in the market (device independent) i.e. application can run in normal browsers, various types of WAP browsers, Voice browsers etc. it should support current and future technology.
- Security – Need for a model that is secure. That is the model should satisfy the five requirements of a secure system ;confidentiality, authentication, availability, integrity, non-repudiation
- Portability – the model should be portable to any platform and system

- Extensibility – The model should be highly extensible
- Scalability- the model should be scalable

Lastly the model should be able to address most of the utility providers challenges which are within the scope of this research project. The challenges we identified through interview and observation and has been highlighted in the analysis section of this report.

Meter reading component can be implemented using WWW model, Secure SMS model and the WAP model. The WWW model cannot be used because of the limitation of mobile devices highlighted in the analysis section. The secure SMS model is not preferred due to the limitation in length, language dependent and lack of interactivity with the data source. This leaves WAP model as the most viable solution albeit with its limitation mainly in terms of security and adaptability. In order to use the WAP model we need a solution for the WAP gap and adaptability shortcomings. The section below discusses the solution to the shortcomings of the WAP model

WAP model shortcomings solution

There are a number of possible workarounds to reduce the risk posed by the WAP gap issue and minimize the possibility of it being maliciously exploited. These include:

- Ensuring the WAP gateways at the wireless network operator's premises are installed within a heavily secured data centre area with very restricted access. The best practice is to install the WAP Gateway at the application server or the web server. Avoid outsourcing the WAP gateway for critical application.
- Designing the message translation process handled within the gateway such that all encryption, decryption and encoding take place within memory without the use of any temp files or explicit writes to disk.
- Ensuring that no details of the translation are ever logged to disk.
- Hosting the WAP gateway within the same secured wired network (i.e. wireless application owner's own network) as the application server and taking full responsibility for its administration. This ensures that all the inter-protocol translation process is done within the wireless application owner's secured network.
- Use of RADIUS server between the WAP gateway and the Wireless provider.
- Another method for securing WAP solutions is by implementing WTLS tunneling. WTLS tunneling is a new technology that eliminates the WAP gap by providing a WTLS "tunnel" within the WAP gateway such that secure messages can be passed from the wireless device through the WAP

gateway and then to the server without being decrypted. In a WTLS tunneling system, the encrypted data from a wireless client-device is sent to the server, just as in a regular WTLS session; however rather than switching from WTLS to SSL encryption, the server sends a new 128-bit WTLS key encrypted with the user's public key. This new 128-bit WTLS key is then used to encrypt data for the rest of the transaction. WTLS tunneling ensures end-to-end WTLS encryption for communications, as data is not decrypted until it reaches its final destination [6]. This solution as been used in the current WAP 2.0 compliant devices.

Proposed solution to WAP Security loop hole

For this project the following viable solutions are recommended for the WAP gap

- Host the gateway within the secure intranet of the corporates server room.
- Use of RADIUS server to enhance authentication of the WAP gateway server

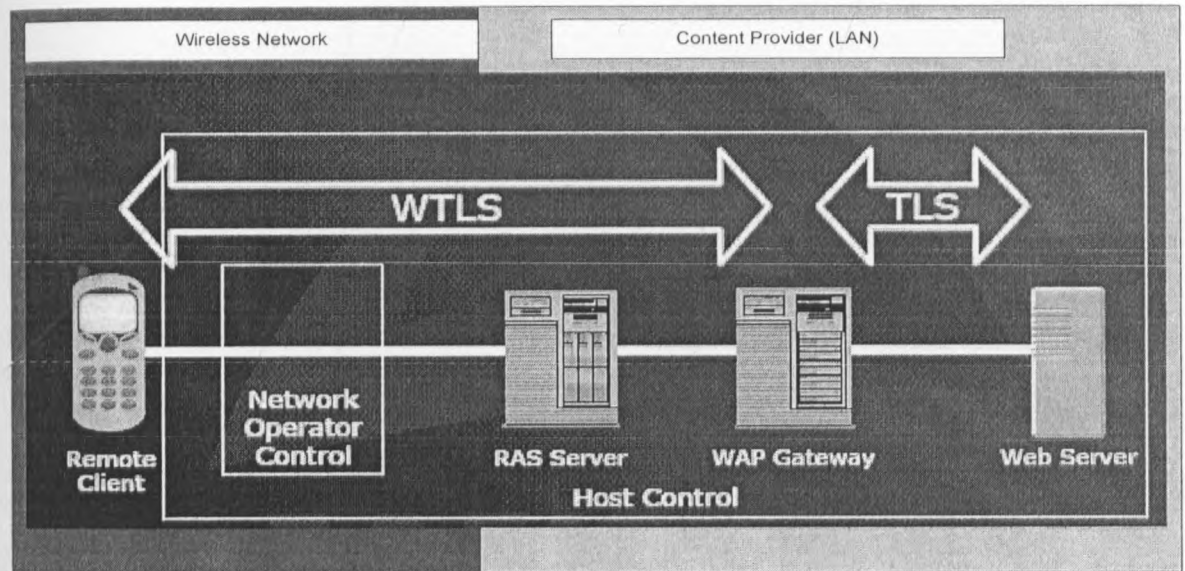


Figure 2.2 Solution to the WAP gap

Proposed solution to WAP Adaptability shortcomings

The reasons why WAP m-commerce is still not popular is the requirement that developers have to develop two similar pages one for the web using HTML standard and one for WAP browsers using WML standard. Another problem is that WML tags vary from device to device hence a page that can be displayed in Nokia might not be displayed in Samsung phone. This creates an irritation effect because of need to test the application in a variety of mobile devices to be confident of variety support. For adaptability there is need to have a device detection component and display content based on the browser in use. This eliminates the need to test the application in a variety of devices and the need to

develop two pages one for WAP and another for web.

Customer Information component can be implemented using WWW model, SMS model. The WWW model used for mailing Statement because of the size and bandwidth required and SMS model for short message information.

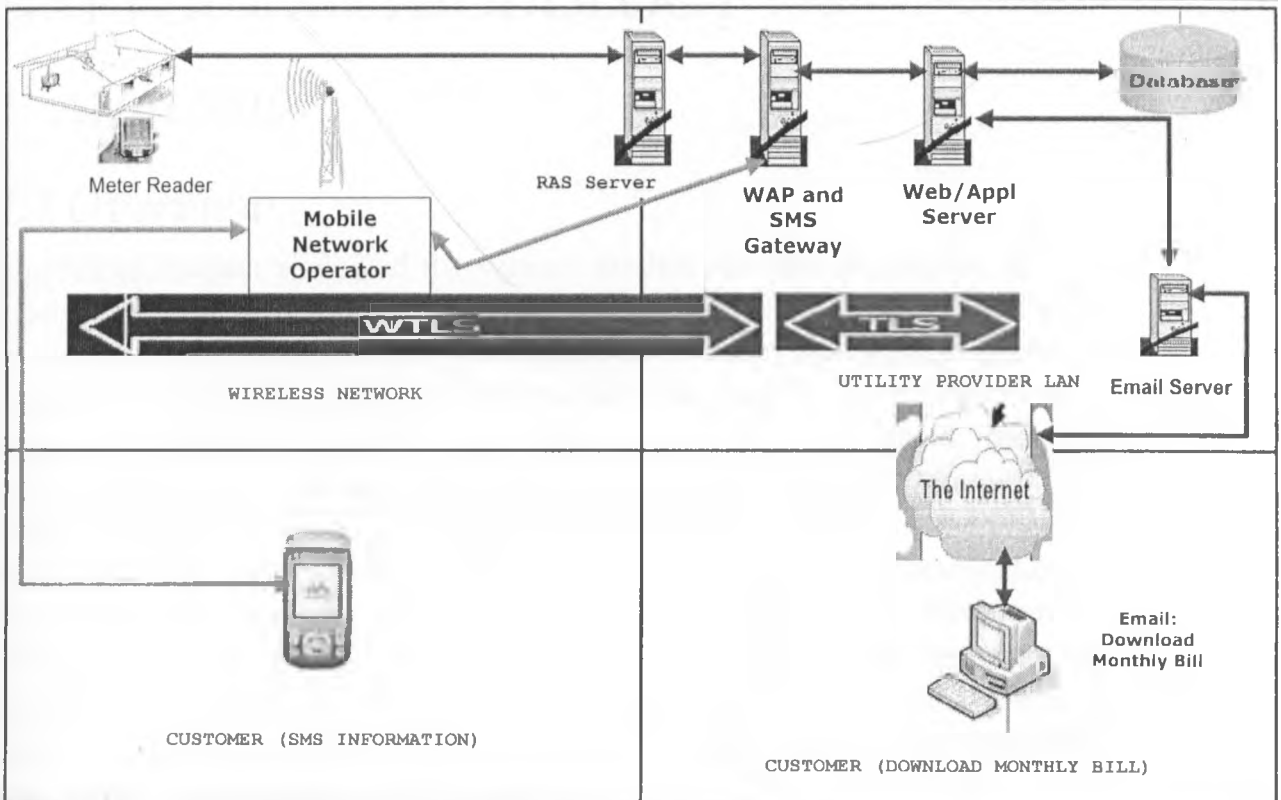
To develop the model we combine three models, the WAP model for meter reading component, the SMS model and WWW model for customer information model. When developing the mobile data collection model the WAP model discussed above was used as the main building block of the model. The WAP model was enhanced by taking into consideration the security loop hole into perspective and correcting it by use of RADIUS accounting server and hosting the WAP gateway inside the utility local area network. The WWW model was used for email services and the SMS model was used for customer information and session establishment. Discussed below are the various main blocks that make up the model. Figure 2.1 below is the proposed model for mobile data collection system for utility providers.

Wireless Network - This is composed of a WAP enabled mobile device, the Mobile Network Operator and the meter. Security is taken care of by the wireless Transport Layer Security.

RADIUS Accounting Server -Mainly included solve the weakness of WAP model when changing from WTLS to TLS or SSL.

WAP Gateway -Used to offer internet connectivity to WAP enabled mobile phones. We used an open framework that can be set up within the local area network of the utility provider to reduce on the cost and make it more secure. To make the system adaptable to any browser due to changing technology and modern mobile phones with operating system i.e. windows CE, we included a module in the WAP gateway to detect the type of the device and render the appropriate technology.

MOBILE DATA COLLECTION SYSTEM MODEL



N/B: THIS MODEL COMBINES THE WAP MODEL, THE INTERNET (WWW) MODEL AND THE SMS MODEL TO COME UP WITH A HYBRID MOBILE DATA COLLECTION MODEL FOR METERING SERVICES. THE WAP MODEL SHORTCOMINGS OF WAP GAP IS ADDRESSED BY THE RAS SERVER AND HOSTING THE GATEWAY INSIDE THE LOCAL AREA NETWORK OF THE UTILITY PROVIDER.

Fig. 2.3 Mobile data collection model

Web Server - It's used to process the scripts and pages and connection to the database server and the Email server.

Database Server - Has the corporate database to stores the data of the corporation.

Email Server - It handles customers mailing of bills and other mailing information.

Customer PC - Download the monthly bill statement.

Customers Mobile - Receive short message service which is mainly informative

CHAPTER 3: METHODOLOGY

3.1 ANALYSIS

3.1.2 Overview

The previous chapter reviewed the various models that can be used to develop this prototype, their weaknesses and enhancements that can be done to make them more secure and usable. We also developed the mobile data collection model based on the integration of three models discussed in the literature review. Taking the challenges faced by the Utility providers into context, the cost, usability, security, adaptability, portability and extensibility into account. The research project will begin by looking at the current operations of the NWC in terms of metering services and using mobile technology and combination of other technologies propose a reengineered cost effective process. Based on the limitation of mobile phones, we will come up with a both functional and non functional requirements for the system. We will then use the model developed in Figure 2.6 that addresses the weakness of the other models highlighted earlier and carry out usability analysis of the prototype.

3.1.3 Methodology used

Literature survey was done to identify the other related mobile metering solutions their weaknesses and strengths. The models that can be used were also researched and analyzed to find their appropriateness.

In order to identify challenges facing utility providers and how current workflow can be reengineered, a fact finding was done at the NWC through interview and observation. The type of questions were structured in such a manner that the workflow and current challenges facing utility providers are captured. The Nairobi Water company was chosen as a representative sample of all the other utility providers in Kenya. It is also important to note that this is a prototype and further survey and analysis is recommended for the system to encompass all the varying factors that have to be considered before system implementation.

Other important information was obtained through observation, journals, books and more importantly the internet. Since WAP is a fairly new technology the internet and journals were the main contributory of information in the development and analysis of the prototype.

Based on the mobile data collection model developed in chapter two figure 2.6 a prototype of the model was designed. In the design of the prototype data flow and flow charting was used to design the prototype.

The prototype was implemented using PHP language with combination of open source technology and MySQL database. In the development we used the modular approach where each module making the model was developed and tested independently. After all modules were developed, the prototype was integrated then tested as a unit to ascertain the workability of the proposed model.

In testing we followed the modular and unit testing approach. Each module was tested independently then integration was done and overall testing was the done as a unit.

Security analysis and usability analysis were done since there are the components determining the viability of the proposed solution. Usability analysis were done by the NWC by performing the experiment described in Appendix E and answering the Survey questions contained in the questionnaire attached in appendix E.

3.1.4 Requirement Analysis

This section describes the requirements for the prototype. Proposes a model for the prototype and also the hardware and software used to develop the solution are described. Finally a description on how the various components of the model work are highlighted.

Review of Current Metering Processes

In Kenya currently there are two main processes of meter reading, the manual process and the Logger (PDA) process. These two methods are used by both the KPLC and NWC. Below is the analysis of the two processes which will assist in the design of the mobile data collection prototype.

Manual process

In this system meter readers are sent to the house of the customer with printouts of the customer account details. The meter reader accesses the meter and records the current meter reading against the customers account; the forms are the

returned branch office. The branch operations officer certifies the forms and sends them to the headquarters for onward transmission to the data entry department. The entry department will then schedule the forms for keying in to the system. Once the forms are keyed in the computer department is instructed to run the monthly billing process. The computer department will then print the customer monthly bills and forwards them to the registry section for grouping and postage to the customer. The process is shown below

Flow chart of the manual process

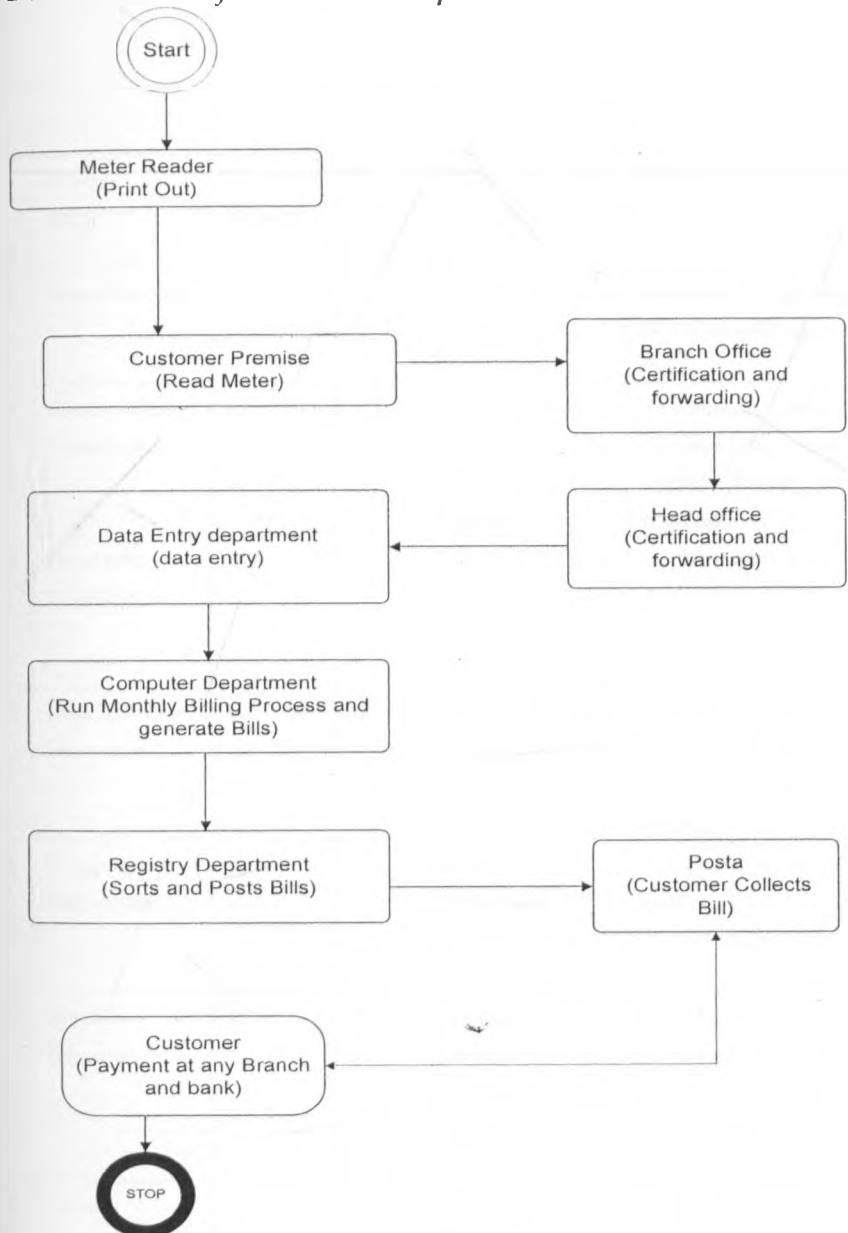


Figure 2.4 Workflow of the manual process

For a manual process it was found out that it takes at least two 34 days from the time the process is initiated to the time the customer gets the bill as tabulated below.

#	Process name	No. of person	Time (days)	Cost elements	Risks	Recommendation	Savings
1	Meter reader gets print out of customer details	2	1	Print out, transport of print out, time of distribution	Print out can get lost, alteration, displacement of forms	This process is not necessary in the proposed solution	All costing associated with this process
#	Process name	No. of persons	Time (days)	Cost elements	Risks	Recommendation	Savings
2	Meter Reading	1	1	Travel to site, writing material	Alteration, eligibility, forms, displacement of forms	Use mobile to post readings. No need of print out	Writing material
3	Branch office Certification	10	5	Consolidated printouts, time of cert, man power	Alteration, Eligibility, displacement of forms, invalid entries, miss postings	This process is not necessary in the proposed solution	All costing associated with this process
4	Head office Certification	20	5	Sorting, time of cert, man power	displacement of forms,	This process is not necessary in the proposed solution	All costing associated with this process
5	Data Entry Department	100	10	Entry, Checking, Print outs	Alteration, Eligibility, displacement of forms, invalid entries, miss postings	This process is not necessary in the proposed solution	All costing associated with this process
6	Computer Department	10	5	Run Billing, Print outs	Displacement of print outs	This process is not necessary in the proposed solution	All costing associated with this process
7	Registry Department	50	10	Sorting, Stamping, Folding, Posting charges	Displacement of Customer Bills, miss postings, no way of confirming acknowledgement	This process is not necessary in the proposed solution	All costing associated with this process
8	Postal Corporation	-	3	Sorting, Stamping, Collection expenses	Displacement of Customer Bills, no way of confirming acknowledgement	This process is not necessary in the proposed solution	All costing associated with this process

9	Customer Payment at branch	-	-	Payment expenses	Customers unwillingness to pay because of lack of efficient system of payment	Integration to mobile Wallet or MPESA.	
---	----------------------------	---	---	------------------	-------------------------------------------------------------------------------	----------------------------------------	--

Table 1.1 Manual process analysis - Process provided by Mrs. Helen Machayo Supervisor (Nairobi Water Company)

Advantages

- Easy to implement.
- Does not require high level of skills to use hence can be used even by unskilled staff.

Disadvantages

- Costly in terms of manpower required to complete the process
- Time wasting takes at least one month to complete the above process
- Double entry errors i.e. no guarantee that the value entered by the meter clerk is the same as that one keyed in by the data entry clerk.
- No way of knowing whether the meter clerk actually visited the customers premise. Currently some of them fake the values.
- The system is not customer friendly.
- Not easy to implement security to secure the data because it has to pass through a number of hands.
- Decision making is not easy

Logger process

In this method the meter reader is given a Logger (PDA) with a spreadsheet containing the customers' accounts. When the clerk reaches the site he enters the current meter reading in the spreadsheet. He will then take the Logger to the branch office where the spreadsheet is downloaded for consolidation then taken to the data entry department for upload to the system.

Flow chart of the process using PDA (Logger)

For a Logger process it was found out that it takes at least two 14 days from the time the process is initiated to the time the customer gets the bill as tabulated below.

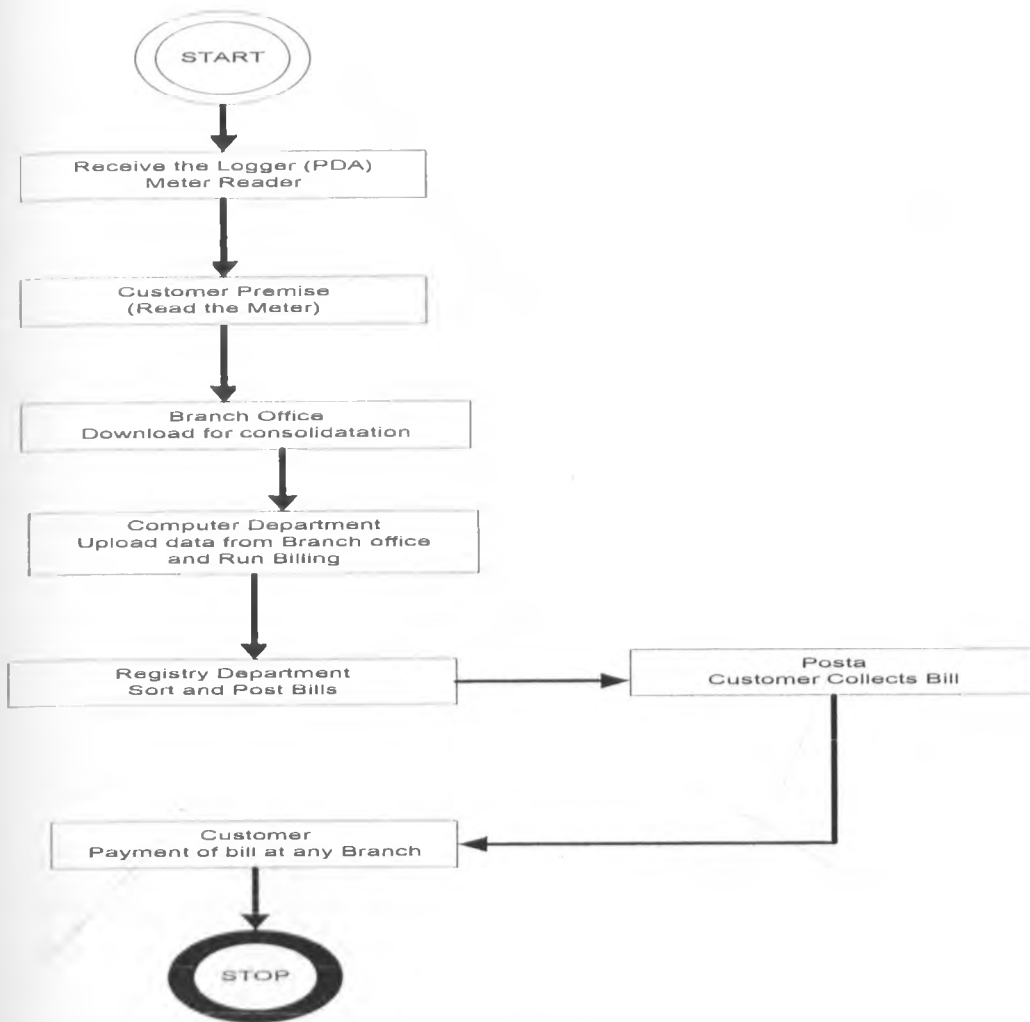


Figure 2.5 Workflow of the PDA logger Process.

#	Process name	No. of person	Time (days)	Cost elements	Risks	Recommendation	Savings
1	Meter reader Logger assignments	2	1	Logger, Print out, transport of print out and logger, time of distribution	Logger can get lost Has no water tight authentication mechanism	No need of a logger or Print outs	All costing associated with this process
2	Meter Reading	1	1	Travel to site,	Alteration	Use mobile to post readings	logger
3	Branch office Download for consolidation	5	1	time of download, man power	Alteration, Eligibility, displacement of loggers, invalid entries, miss postings	This process is not necessary in the proposed solution	All costing associated with this process

4	Computer department Uploading And billing	20	2	time of download, man power	Alteration, Eligibility, displacement of loggers, invalid entries, miss postings, Displacement of print outs	This process is not necessary in the proposed solution	All costing associated with this process
5	Registry Department	50	10	Sorting, Stamping, Folding, Posting charges	Displacement of Customer Bills, miss postings, no way of confirming acknowledgement	This process is not necessary in the proposed solution	All costing associated with this process
6	Postal Corporation	-	3	Sorting, Stamping, Collection expenses	Displacement of Customer Bills, no way of confirming acknowledgement	This process is not necessary in the proposed solution	All costing associated with this process
7	Customer Payment at branch	-	-	Payment expenses	Customers unwillingness to pay because of lack of efficient system of payment	Integration to mobile Wallet or MPESA.	

Table 1.2 Logger process analysis - Process provided by Mrs. Helen Machayo Supervisor (Nairobi Water Company)

Although the process as been reduced to seven processes it still takes an average of 18 days for the customer to get the monthly bill and the man power required is still unnecessarily high. It has also several security loop holes like alteration of data and identification of where the alteration occurs remains a challenge.

Advantages

- Reduces double entry associated with the manual system
- Reduces the time taken to complete the process
- Does not depend on any connectivity hence quite reliable

Disadvantages

- Extra work of uploading the data into the system.
- Not extensible
- Bulky to carry the device around
- Not easy to implement security features required
- Data in the spreadsheet has to be formatted in a strict manner.
- Does not significantly reduce the time required to serve the customer.

- Need to verify entries before batching them to the central system
- Not adaptable to other hand held devices.
- The device is very expensive to maintain and purchase. It goes for average of Kenya Shillings 130,000.00 and annual maintenance of 25,000.00.

Data capture challenges facing utility providers.

Utility providers face quite a number of challenges in reengineering their metering services to make them more efficient and cost effective as we found out from our interview with the supervisor of the NWC. A look at the operations of the NWC, we found out that they face the following challenges

- Reducing the cost operations related to meter reading and customer information
- Timely meter reading and sending of bills to the customers
- Increasing accuracy in meter reading and subsequent updates in the system
- Ensuring that the meter readers actually visit the site and get the correct values
- By-passing of metering by crooked customers especially in disadvantaged estates
- Availability, reliability and convenient way of payment of bills by customers
- Getting a metering solution that is cost effective, adaptive, secure, portable, extensible and usable in the market
- Enhancing security of the customer data and the metering equipment.
- Problem encountered when visiting customer premise i.e. closed gates, Dogs etc
- Invalid readings leading to approximation of the meter reading and a customer paying twice in a circle. A good example records available for a customer of KPLC is that the meter reader in June 2008 enters a reading of 13100 instead of the actual 12925 and in the next month of July 2008 the meter reader realising the meter reading is still at 12976 decides to reset both the meter reading previous and current to 12976. The customer although he had paid up to 13100 has to start again to pay extra 124 units he had paid for.

Although the proposed solution will not solve all the challenges highlighted above but will go a long way in addressing quite a number of them. Further enhancement of the system to include geographic position services and branding

of meters with an encrypted barcode which will be transferred to the mobile phone as a picture and processed using the imaging processing module will go along way to solve the above challenges.

Requirements for a M-solution

Unlike desktop computers mobile devices have various limitations that have to be taken care of when designing applications meant to run on this devices. Its important that that this limitation are are addressed. Below are the challenges that need to be addressed when designing M-solutions.

Limitation of mobile devices

The first challenge is to bridge the limitation of mobile devices in order to be usable; mobile phones have to be small in size and light in weight. This puts rather severe limits on their design, which results on several challenges:

- The battery has a fairly low capacity, resulting in more limitations due to having to keep power consumption down for every part.
- They have small screen and keyboard, resulting in very limited input and output possibilities and making user interfaces awkward.
- Slow processor and little memory, resulting in little computation being possible on the phone itself. Some of these limitations apply only to phones and other mobile devices do better. For example, the screen size of a Palm device is large enough that simple text processing is doable. For every device meant to be mobile, however, the limitations will apply to some extent. It is not really possible to comfortably carry around a full size keyboard, mouse, and screen.
- The wireless mobile network also has severe limitations, compared to a wired local area network. The total amount of bandwidth that all mobile users in a geographical area can share is limited. With cables it is always possible to expand the bandwidth by installing more cables, but the total spectrum of radio waves available for mobile networking is limited both by physics and by the way it has been allocated to various purposes by governments.
- Radio waves are also inherently error prone, since they are affected by many sources of disturbances: other devices and the Sun cause interferences by sending their own signals, and buildings, mountains and other parts of the landscape distort and in some cases prevent the radio signals from reaching their destination. Even if nothing else is a problem, the distance to the nearest base station for the mobile network may be too large.

- This results in a network with limited bandwidth and a high error rate. Normal networking protocols, such as TCP/IP, have been designed for an environment with low error rates, which makes them partly unsuitable for a mobile network.
- Additionally, the various protocols used in the Internet (and that's about the only interesting global network for mobile users as well) on top of TCP/IP are textual, meaning that the messages they send are plain text. This makes them easier to specify and understand, and much easier to implement them and debug the implementations, but when bandwidth is very limited, they do waste it.

Usability

The second challenge is to make the applications easy to use and at the same time allow consistent, always available access to relevant data, even when network coverage is not available. For mobile phones users can register more than one provider such that in case the primary one is down they can switch to the secondary one.

Network security

The third challenge is the network security. The data sent and received should never be exposed en route between the user and the corporate firewall even when using different networks and technologies. Only a VPN solution provides a truly network independent solution as different wireless network technologies have their own distinctive security features and characteristics and vary from insecure to almost secure. For extremely confidential information the security of wireless networks is not enough without network independent solutions like VPN. Also the security should be enforceable from a central, administrative console to ensure compliance.

Unreliable networks

The fourth challenge to overcome is the network reliability. The lack of high-speed and robust wireless networks necessitates a mobile application solution that minimizes network reliance, optimizes data transport, and mitigates the disruption from dropped connections. For the design of the applications this means that the most critical information exchanges should be designed to be carried out in the narrowest band network used for the application and that only the most critical information is transferred. Disruptions and errors can be handled by applying techniques to ensure the integrity of the data transferred.

Scalability

The fifth challenge is scalability. The proliferation of wireless devices and mobile applications creates an immense administrative burden on corporations. To

attain their full return on investment, even large-scale solutions must be completely and easily manageable by just few centrally-located administrators. For these management and also security reasons it is reasonable and recommendable to separate corporate mobile users to a separate sub network with their own firewall and servers. To cut down the amount of wasted time it is also important that the users could update their user profile, device profile, or mobile application suite on the road without having to return to the office. All the necessary updates and data synchronization should be able to be done on-the-air as requested as the device is connected to the network. Security updates would have to be forced so that the users could not avoid them. This way also a stolen or lost device could be locked up as it enters a network.

Enterprise integration

The sixth challenge is to integrate the mobile applications to existing enterprise systems. Mobile applications must be able to access all relevant corporate data and still fit seamlessly into existing corporate infrastructures. Enterprise legacy systems and databases are adaptable to new forms by using middleware solutions: the information on old databases can be converted to XML format, which is then easier to refine and reform to other forms. Middleware can also be used to recognize the user's (mobile) device and its capabilities and then reform the data into a form the device can understand. The same thing can also be done vice versa when the user sends information back to database from the device. This is called adaptive infrastructure.

Extensibility

The seventh challenge in wireless applications is the extensibility. Solutions or applications should be adaptable to changing needs: they should be able to evolve as business needs to evolve. Extensibility is best achieved by applying open standards. Currently open source technology is fast becoming as a standard in mobile computing and mobile applications.

Information system security

The last challenge in mobile applications is to ensure that the systems are secure and only authorized users access the system. With the rapid growth in e-commerce and m-commerce, the security of sensitive information being transmitted over an open network like the Internet and mobile internet, has continued to be a serious cause for concern.

The goal of a good, reasonably secure information system is to always ensure that the following five basic tenets of information security are all well accounted for in the infrastructure, procedures, policies and people associated with its deployment:

- **Authentication** – the process of validating the true identity of a user requesting access.
- **Authorization** – the method of establishing the rights and privileges of a user during its interaction with the system.
- **Confidentiality** – the means of ensuring that all sensitive data being transmitted can only be read by authorized parties.
- **Integrity** – the process of preventing alteration of data in transit by unauthorized third parties.
- **Non-repudiation** – the means of proving the occurrence of a transaction and making it impossible for parties involved to deny carrying out the transaction.

Various standards and protocols have been put in place to ensure support for the above security requirements within the wired Internet infrastructure. These include SSL (Secure socket Layer), TLS (Transport Layer Security), S-HTTP (Secure HyperText Transport Protocol), Public-Key Cryptography, use of Digital Certificates and Digital Signatures etc.

However, these technologies by the nature of their design can only be implemented over the wired Internet since it provides the required high bandwidth, low latency and stable connections with client machines having a comparatively higher processing power. Due to the absence of these features in the wireless networks, these security standards could not be applied directly onto the wireless Internet without modification. The Wireless Application Protocol (WAP) was designed as a lightweight protocol to enable communication between resource-constrained wireless devices and the wired Internet.

User Requirements

To conceptualize a mobile application, additional informational added values have to be targeted, using mobile added values. In other words, it is far from sufficiency to just porting an existing Internet application on a mobile device. Mobile applications have to be specifically made-to-measure on the one hand side to the needs and expectations of the mobile user, and on the other hand side to the specific restrictions of mobile communication techniques and mobile devices.

In order to derive a set of requirements to mobile data collection system we pursue two steps: Firstly we identify general characteristics of the mobile use which are relevant. Secondly we closely watch the user and his context when wanting to use mobile data collection system.

Characteristics of the mobile use

The use of mobile applications underlies several specific restrictions. We consider five characteristics of the mobile use to be particularly relevant as they greatly influence the design of mobile data collection system and the suitability of certain technical solutions.

- A mobile application is used via a mobile device. For these devices (currently either a mobile phone or a PDA), special limitations are valid. For the mobile data collection system context, above all, these are the limited input and display capabilities.
- The connection is provided by a mobile network operator (MNO). This is especially important if applications need to access certain parts of the infrastructure which are under control of the MNO (e.g. the SIM card). In the case of negotiations, these have to be pursued with all MNO on the designated market.
- The use of mobile data transmission is expensive. In the case of circuit-switched data transmission (e.g. GSM) this extends to the connection time, in the case of packet-switched data transmission (e.g. GPRS) this extends to the transferred data volume.
- Sensitive data is transmitted. This implicates the use of adequate security measures.
- A disruption of the usage is possible at any time. This is principally already true for electronic data collection system as well (the connection may e.g. be disrupted by a breakdown of the transmission or of the operating system of the client computer) and provides a special necessity to avoid incomplete transactions. For mobile data collection system, it is extremely more probable as a mobile usage causes a continuous change of conditions, e.g. through geographical influences or cell-handover. Thus, it is also important for the usability of a service.

It is important that the named restrictions have to be considered as early as possible, which means in the phase of conceptualization.

Resulting requirements

With regard to the characteristics we identified and the use cases we introduced we develop 15 requirements to mobile data collection system which are explained in the following.

The requirements can be discerned into four categories: technical, usability, design and security. We did so in order to later locate the problem areas of applications.

Technical requirements:

- The usage must be possible with both kinds of available mobile devices. This requirement is resulting from the characteristic that usage will be made with a mobile device. It should be possible for the user to use his preferred device, in order to benefit from its advantages.
- The application should adapt to the conditions of the mobile device automatically. This is resulting from the same characteristic. The application should automatically detect the kind of device it is executed on and adapt automatically to its features.
- The usage must be possible for customers of any MNO. This requirement results from the characteristic that usage will be performed through the network of one the respective MNO. The usage must be possible for everybody; the customers of one operator must not be locked out.
- The amount of the transmitted data should be as small as possible. This requirement results from the second characteristic that mobile data transmission is expensive. Additionally to the aspects of cost, the aspect of waiting time (impacting negatively on convenience) for the transmission is also important.

Usability requirements:

- This requirement results from the fact that mobile data transmission is expensive (this especially for circuit-switched connections) as well as from the fact that a disruption is possible at any time. It should be possible to use the application without a permanent connection to the server.
- A simplified method of data input. This requirement is of special interest when a necessity is given to enter request through voice instead of typing or ensure it accepts valid keys only.
- "One-Click"-Request of important data. It is important to allow quick access to information. This information should be available with just a few "clicks", in the ideal case with only one.

Design requirements:

- The possibility to personalize the application. This requirement can be deduced from different use cases. If the user gets a lot of data displayed, there should be a possibility to use a personalized structure to view the data.
- The possibility to scale the application. This concerns the easy switch of use cases for the user, e.g. if he gets an unexpected account number and

wants to find out more details. In these cases, it should be easily possible to switch to a version of the application with a wider range of functions.

- The possibility to get announcements on important events. In some use cases, especially in the control of account movements, it makes sense if the application could provide push functionality. Also URL should be pushed to the meter reader on authenticating the session.

Security requirements:

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

Application Specific Requirements:

- The personnel involved directly in the posting of data should be the remote originator (Meter Reader).
- The posting of the meter reading should trigger all the processes within that entity and at the end of the process the customer should be having the monthly statement on his mail box.
- The process should be reduced to a very short time i.e. not more than 10 minutes.
- The cost of transaction should be kept as low as possible.

3.2 DESIGN

3.2.1 Prototype Design

The prototype design is based on the developed model in chapter 2 figure 2.6 A web interface will be developed linking to the companies' central database that manages customer billing records. This system will be accessed via the mobile devices using the WAP protocol. The WAP gateway will be responsible for decoding and encoding the information such that the system can run in mobile

devices which are known to have various limitation discussed earlier. The WAP gateway will also be enhanced to work as a SMS gateway such that the customer can use to query the system for various functions for example checking current balance and ordering Monthly statement.

The major milestone of this project is to cut down on operational cost while enhancing efficiency, a module for generating a PDF statement and emailed to the customers will be developed. The generation of the customer's statement will be triggered by an update of the customer records via the mobile devices. This will eliminate the monthly printing and postage of customer bills and statements. Security will be enhanced at the WAP and SMS gateway such that the WAP gateway will be developed in such a way that a part from checking the conventional way of logging in, only authorized mobile phones can access the system for those updating the meter reading.

Flow chart of the proposed solution

The above two methods of meter reading which are currently in use simultaneously requires reengineering to reduce on time of the entire process to one day, improve on security of information and reduce on the number of personnel involved in an entity customer transaction to one. In this prototype we try as much as possible to reduce human interaction with data and let only a single user be responsible with the entire customer transaction from meter reading to sending of customer bill. The following diagram figure 2.6 shows the flow chart of the proposed reengineered process.

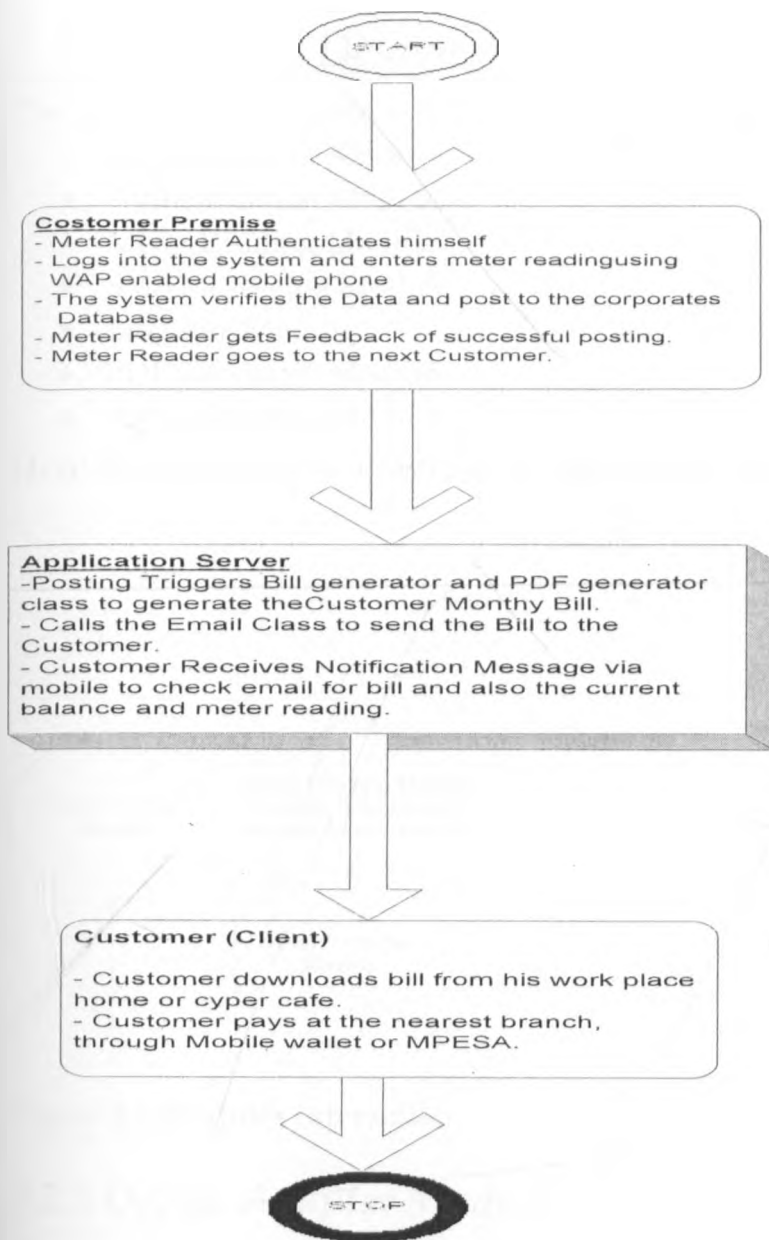


Figure 2.6 Workflow of the proposed solution.

The process is reduced into two steps with no paper one involved and only the meter reader and the customer involved. There are no players in the middle rather than software services that interact seamlessly to reduce the time from the average 14 days to an average of 10 minutes to receive the bill. Efficiency can further be achieved on the side of payment pay integrating with the mobile wallet such that customer can make payment through credit cards via mobile phone or integrate it to the popular Safaricom MPESA.

3.2.2 Detailed Design of the prototype

The system can be broken down into six main modules

- Device adapter Module
- Authentication Module
- Meter Reading Module
- SMS Messaging Module
- Emailing Module
- PDF Generator Module
- Administrative Module

Here is a systematic diagram to show how the modules interact.

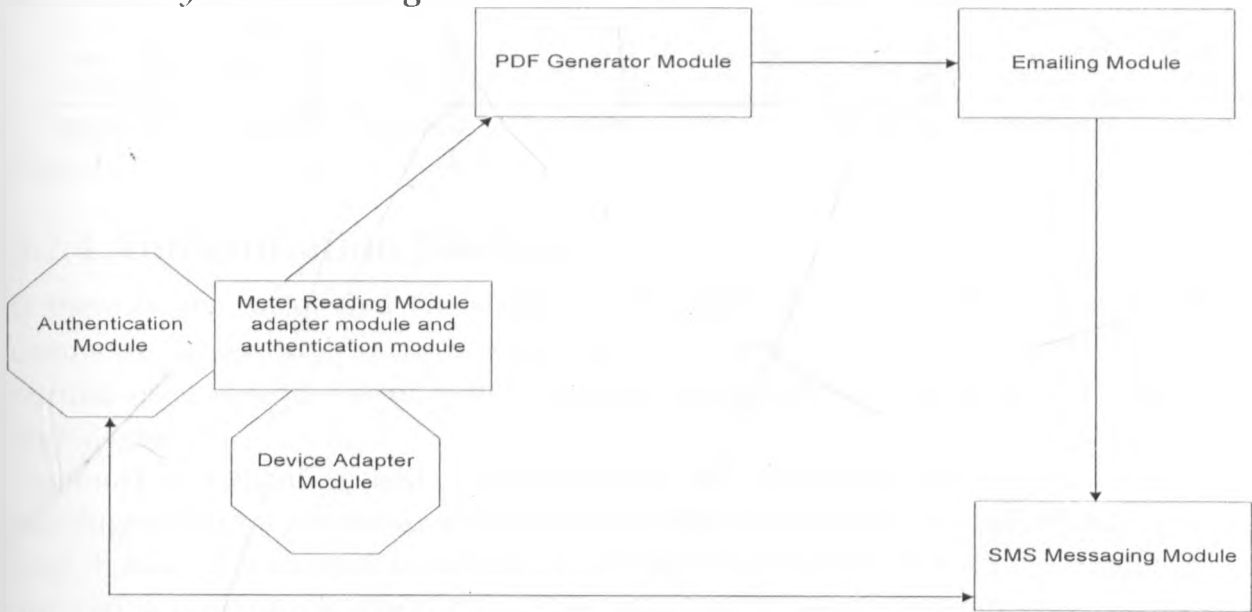


Figure 2.7 Modules interaction

3.2.3 Device Adapter Module

One of the researches of this project is adaptability. There was needed to make the system adaptable to any device the organization might choose to use. In order to achieve this open source PHP library called HTML And WML Hybrid Adapted Webserver (HAWHAW) was used.

This was integrated with the open source WAP gateway to make the gateway device aware and adapt accordingly.

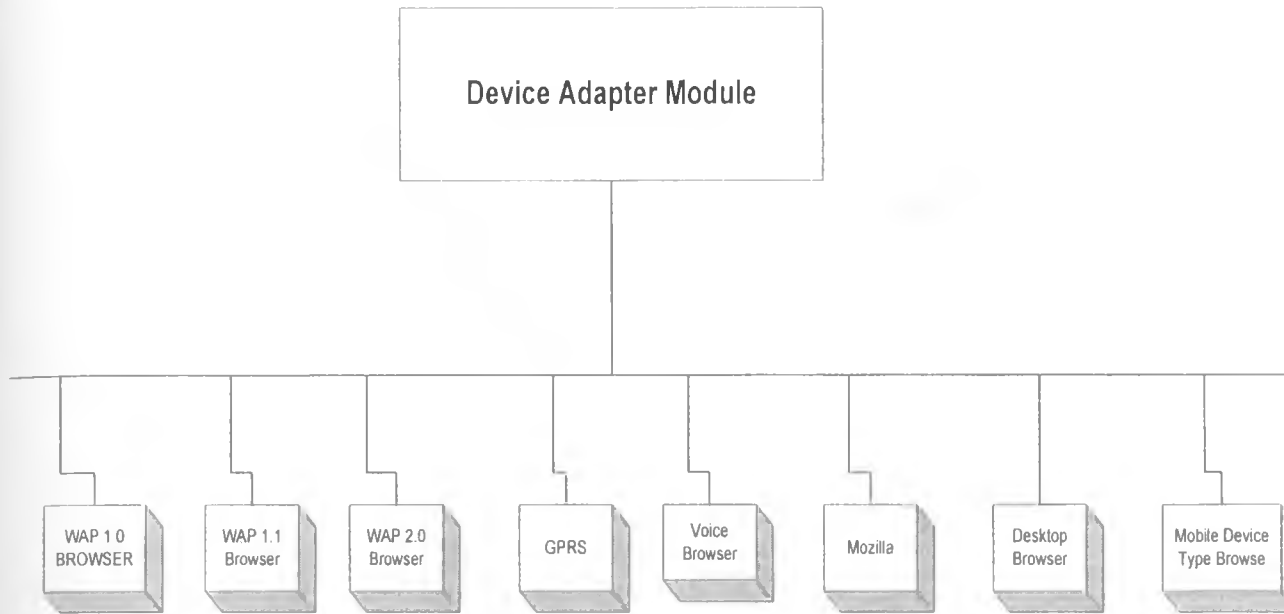


Figure 2.8 Device Adapter Module

3.2.4 Authentication Module

If there is one factor that has hindered the adoption of e-commerce and m-commerce is security. There is need therefore to convince both experts and normal users alike that security that has been implemented in a system is of very high degree.

The most traditional method of authentication has been password, but research has shown that for e-commerce and m-commerce there is need to establish a two way channel of communication is the most preferred method. The session should also last as short as possible and one time password is the most preferred.

In this project the following authentication mechanism were used.

- Establishment of a two way authentication channel, where the meter reader request a session via an SMS message. Note that the channel that SMS Message follows is different from the WAP or internet model. The user will send his credential like the payroll number to the gateway which will trigger the gateway to verify the employee, the mobile number and whether he was authorized to be in the field that day. In this case the mobile acts as like a credit card or ATM. If authorized the system will open a session for a short period of time like 10 minutes for the user, generates a session ID security code by using md5 algorithm and pushes the URL of the meter reading module page to the requesting user using the push facility of the gateway so as message appears as a service for the user to access.

- Due to the limitation of mobile phones the need to minimize clicks is very important. The page will require the user to enter is PIN, the account number and meter reading then click on the submit button. The system will check the security code, the status of the secession and if valid checks the PIN and mobile identification code from the headers and if successful post the data to the central database and closes the session. In real implementation, on the WAP server the configuration file is designed in such way that request are rerouted to the RADIUS server for authenticating the user. RADIUS server is a proven technology for authenticating remote users. RADIUS is also used to seal the WAP gap discussed earlier.
- If the user does not transact within the time given, the session closes and notified via SMS or GPRS message of the same

Below is schematic flow chart diagram showing authentication routes for the prototype

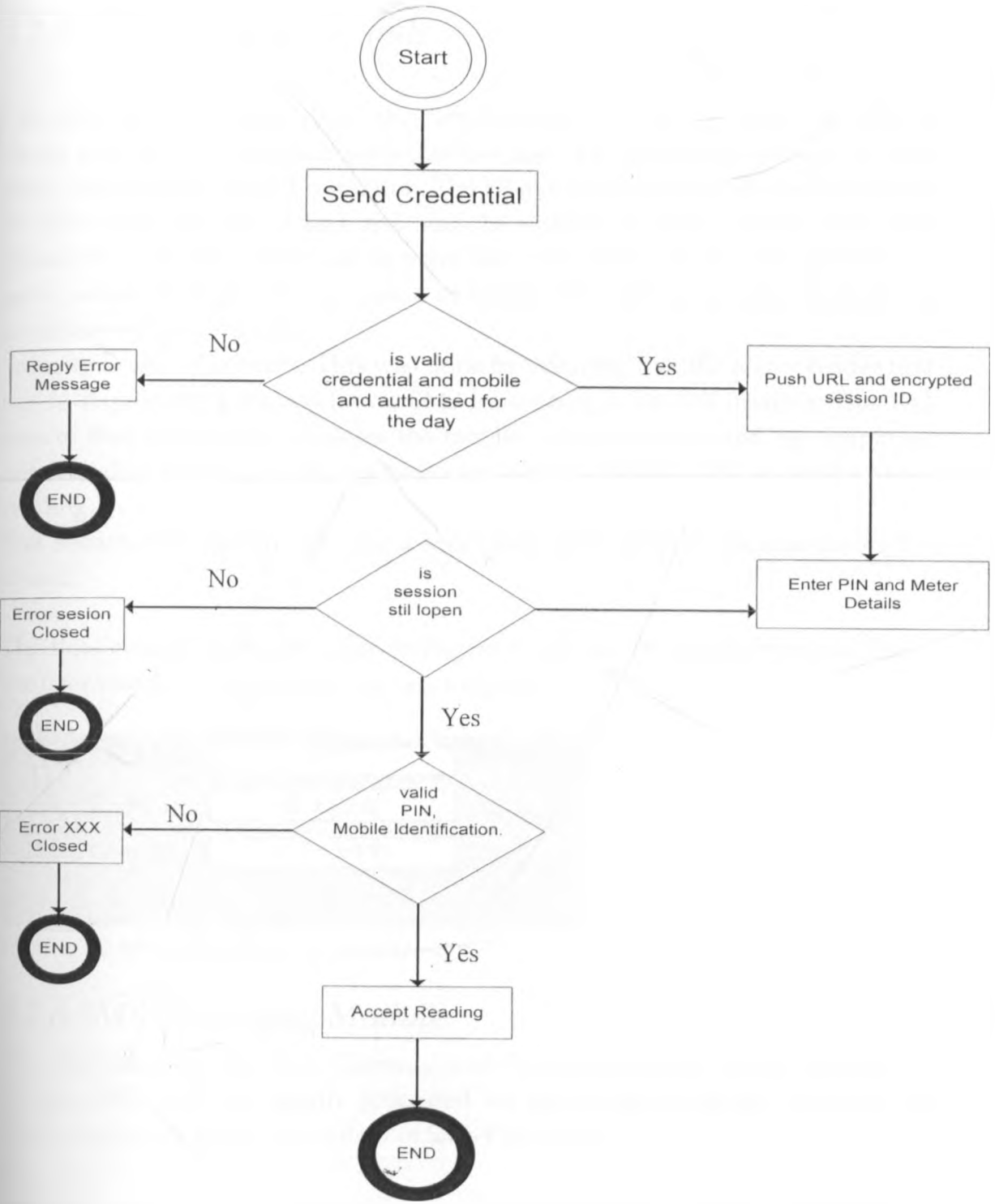


Figure 2.9 Flow Chart Authentication Module

3.2.5 Meter Reading Module

Considering the limitations of the target client devices, the User Interface of meter reading was designed such that the need for substantial amount of data entry was kept to a barest minimum. The UI design minimizes the need for users to enter long streams of text and also the module is voice enabled such that incase the company subscribes to voice data; the meter reader will just have to enter values through talking instead of typing. The values are also validated to avoid entering wrong data.

Security is also of concern. This was done by ensuring that the Meter reader first has to request for a session ID via SMS by sending is payroll number. This will ensure that the system validates the mobile number details and the employee details before pushing a URL via GPRS for login and submission of current meter reading.

The session will remain open for a short time preferably 10 minutes before it's closed.

The flow chart is shown in diagram Figure 2.6 above. The diagram below shows the user interface of the meter reading module

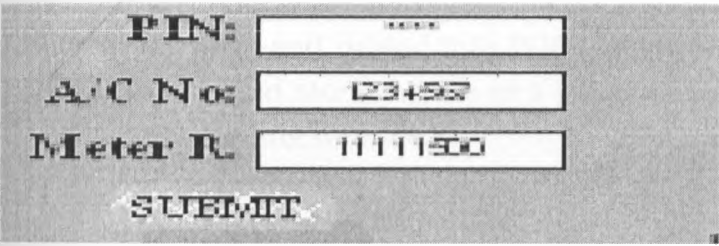


Figure 3.0 Meter Reading Module Design

3.2.6 SMS Messaging Module

This module uses the SMS Gateway which comes with the WAP gateway to process SMS. SMS are mainly processed via the configuration file and they are database driven. Below is the flow of SMS Processing

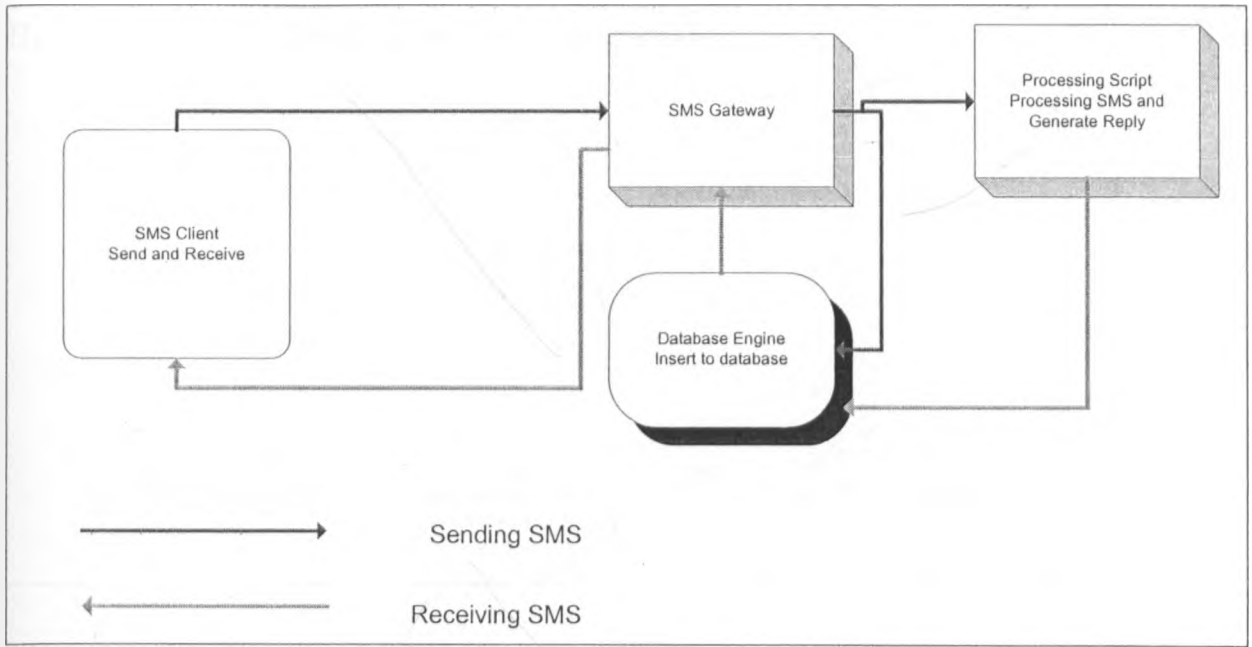


Figure 3.1 SMS Data flow diagram

3.2.7 PDF Generator Module

When the reading is posted into the database, a PDF generator module is triggered. This module will call the individual billing function for the customer and compute the balance and generate the statement. The statement is formatted has a HTML page and passed into PDF generator class to convert the HTML to PDF document and store the file in a temporary file for attachment to email, It the calls the Emailing module.

3.2.8 Emailing Module

The Emailing module will call the send email function and retrieve the customer email information. It will then attach the statement to the Email and send it to a valid email address. The module has an email validator to make sure that email is end to an existing email address. It will then update the status of customer information accordingly

Below is a flow chart of the resulting system

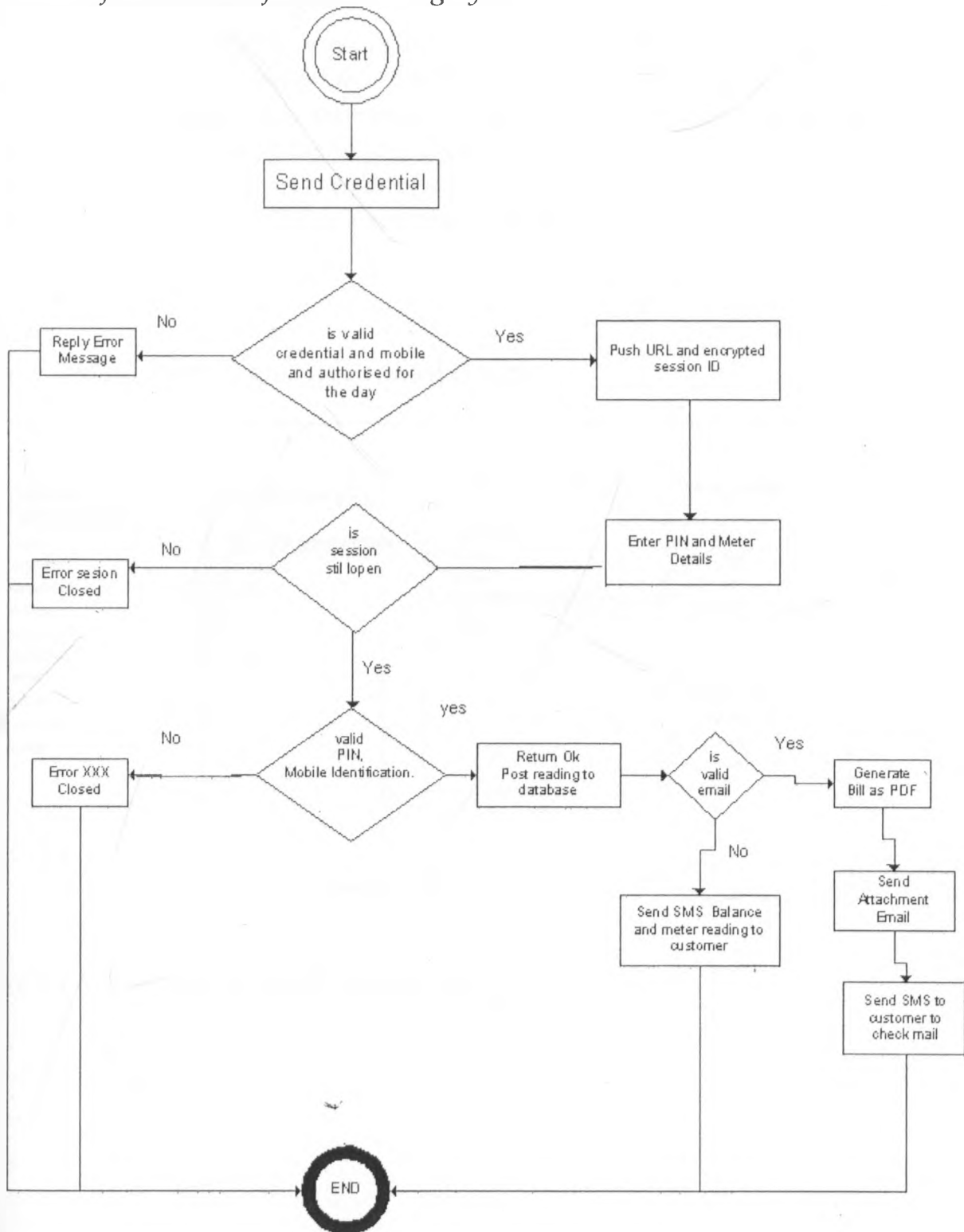


Figure 3.2 Flow Chart of the proposed Prototype Design

3.2.9 Database Design:

In the design of the database most of the tables are simulations of the existing billing system which is expected that the proposed prototype will be integrated. Hence tables like employees, customers, Transactions and meter reading are simulations and will inherit the billing database structure currently in use. For completeness of the prototype the tables are created as simulations and no effort is made to normalize them but concentration is made on the functionality of the prototype.

Figure 3.3 Meter Reading Module Database Design



Figure 3.4 Administrative Menu Database Design

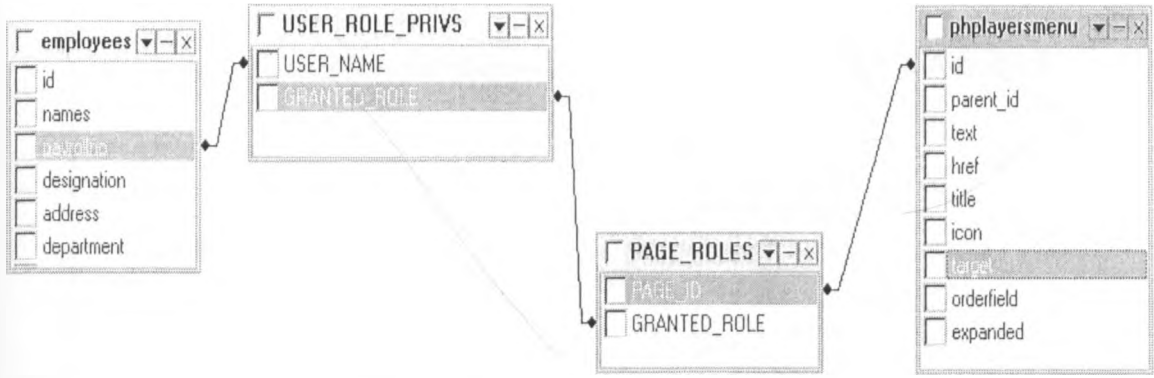


Figure 3.5 SMS Messaging Module Database design

Sending SMS

Receiving SMS

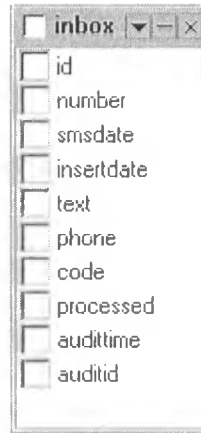


Figure 3.6 Customer Monthly Statements Database Design

customers	
<input type="checkbox"/>	names
<input type="checkbox"/>	accountno
<input type="checkbox"/>	meterno
<input type="checkbox"/>	address
<input type="checkbox"/>	location
<input type="checkbox"/>	mobilenr
<input type="checkbox"/>	email
<input type="checkbox"/>	status
<input type="checkbox"/>	audittime
<input type="checkbox"/>	auditid

transactions	
<input type="checkbox"/>	id
<input type="checkbox"/>	employeeid
<input type="checkbox"/>	customerid
<input type="checkbox"/>	processed_date
<input type="checkbox"/>	insertdate
<input type="checkbox"/>	trans_type
<input type="checkbox"/>	amounts
<input type="checkbox"/>	security_code
<input type="checkbox"/>	sessionid
<input type="checkbox"/>	audittime
<input type="checkbox"/>	auditid



CHAPTER 4: PROTOTYPE IMPLEMENTATION

4.1 Overview

In this chapter we present the implementation of our prototype. We start by describing the choice of technologies used then the system development specifications and the development environment then discuss the design, prototype Implementation and testing. In the implementation of the prototype the following are discussed

- Coding –Explanation of coding is done sample code functions are attached as an appendix
- Testing – Modular and unit testing is done to prove the workability of the proposed solution
- Installation – installation is attached as an appendix
- Documentation –user documentation is also attached as an appendix

4.2 Choice of Technologies Used

Programming Language

PHP programming language was preferred in the development of the prototype because of experience we have in developing application using PHP, its robustness and portability to various platforms. It is also easier to call and manipulate the gateway in PHP.

Mobile Development Framework

The development of WAP enabled application pages is usually in WML and WML Scripting. This could have necessitated learning new technology and syntax for WML coding. To encapsulate this, we used the HAWHAW development framework such that coding of WAP pages is done through the HAWHAW methodology and syntax which is purely PHP standard hence benefit from our wealth of knowledge in PHP programming. HAWHAW is an open source framework for development of web and WAP pages using PHP language which are device and browser independent hence ensuring application adaptability to any device and browser.

The current situation out there is that many WAP applications are highly incompatible and not able to inter work with different mobile devices. This is mainly caused by strong differing browser implementations and network

configurations. Starting to program WML means to painfully learn about all those pitfalls one by one and day by day.

Using this framework the application was developed to be voice aware application such that using voice browsers sound can be used instead of typing and keying in data.

Gateway

The Kannel WAP and SMS Gateway were chosen first and foremost is that it's 2 in 1, have both the WAP and SMS Gateway. Secondly it's a free open source hence has no cost implication meeting our target to develop a cost effective solution. Thirdly, given that what is downloaded is actually the source code for compilation, it can be customize to suite specific needs of the customer. Another advantage is that its development in C language makes it very efficient and fast and suited for large organization processing thousands of records per minute. Given that configuration file is developed outside the kannel it's highly dynamic and portable to any system within the Linux environment. Lastly other boxes can be developed and ported into it for example I integrated with the sqlbox to directly insert SMS to database and pull and send SMS from database without any processing script.

Platform

The Linux environment was chosen because of its support to open source products and resilience to viruses so it further boosts the security of the system. It was also dictated by the gateway chosen which can only run in Unix environment.

Database

MySQL Database was chosen because it free and easily available. The open source nature of MySQL makes it adaptable to many platforms. However it's important that any relational database can be used. On real application implementation the relational database currently in use within the organization will be used with no modification of the source code since connection is provide using ADO connection which is database independent.

4.3 Setting the Development Environment

A development environment is made up of tools, underlying APIs and the operating platform necessary for developing the applications. Developing mobile data collection system using Open source Technology required the following:

- Linux Operating System (Red Hat Enterprise 5.0)
- Apache 2.2.8
- PHP 5.2
- Perl 5.8
- MySql 5.1.5
- Kannel 1.4.1 SMS and WAP Gateway source code
- HTML And WML Hybrid Adapter Web server
- GSM Modem (USB Edge GPRS Modem)
- Mobile Device Simulators

Configuration of the Kannel SMS and WAP Gateway

The kannel SMS and WAP gateway is an open source gateway written in C. its Installation and configuration is a bit complex. After Compiling and installation of the Kannel a configuration file is developed based on the kannel syntax.

Coding Configuration File

A configuration file consists of groups of configuration variables. Groups are separated by empty lines, and each variable is defined on its own line. Each group in Kannel configuration is distinguished with a group variable. Comments are lines that begin with a number sign (#) and are ignored (they don't, for example, separate groups of variables).

A variable definition line has the name of the variable, and equals sign (=) and the value of the variable. The name of the variable can contain any characters except white space and equals. The value of the variable is a string, with or without quotation marks (") around it. Quotation marks are needed if the variable needs to begin or end with white space or contain special characters. Normal C escape character syntax works inside quotation marks.

Perhaps an example will make things easier to comprehend:

```

1 # A do-nothing service.
2 group = sms-service
3 keyword = nop
4 text = "You asked nothing and I did it!"
5
6 # Default service.
7 group = sms-service
8 keyword = default
9 text = "No services defined"
```

The above snippet defines the keyword `nop` for an SMS service and a default action for situation when the keyword in the SMS message does not match any defined service.

Lines 1 and 6 are comment lines. Line 5 separates the two groups. The remaining lines define variables. The group type is defined by the group variable value.

Kannel Boxes

For Kannel to work the configuration file should define the following boxes

- bearerbox – Required in all cases
- sqlbox (Optional if not database driven)
- smsbox – required for SMS facility
- wapbox – required for WAP services

Refer to appendix B: for the configuration file we developed for the application

Running Kannel

To start the gateway, you need to start each box you need. You always need the bearer box, and depending on whether you want WAP and SMS gateways you need to start the WAP and SMS boxes. If you want, you can run several of them.

Starting the gateway

After you have compiled Kannel and developed the configuration file for your taste, you can either run Kannel from command line or develop start up daemons scripts to use it as a daemon

To start the bearerbox, give the following command:

```
bearerbox -v [log level value(0-4)] [config-file]
```

The `-v 1` sets the logging level to INFO. This way, you won't see a large amount of debugging output (the default is DEBUG). `[config-file]` is the name of the configuration file you are using with Kannel.

After the bearer box, you can start the WAP box:

```
wapbox -v [log level value(0-4)] [config-file]
```

or the SQL box:

```
sqlbox -v [log level value(0-4)] [config-file]
```

or the SMS box:

```
smsbox -v [log level value(0-4)] [config-file]
```

4.4 Development of the Prototype

Each module was developed independently then linked to form the complete prototype. Below is the description of the various modules implementation

4.4.1 Device adapter Module

The module is implemented by the hawhaw PHP framework and called before at the top of every WAP page to over adaptability and device independence. It also makes the application voice enabled such that if the browser is voice enabled it calls the voice vxml file. Figure 3.6 below shows the implementation of device adapter module in the design of meter reading.

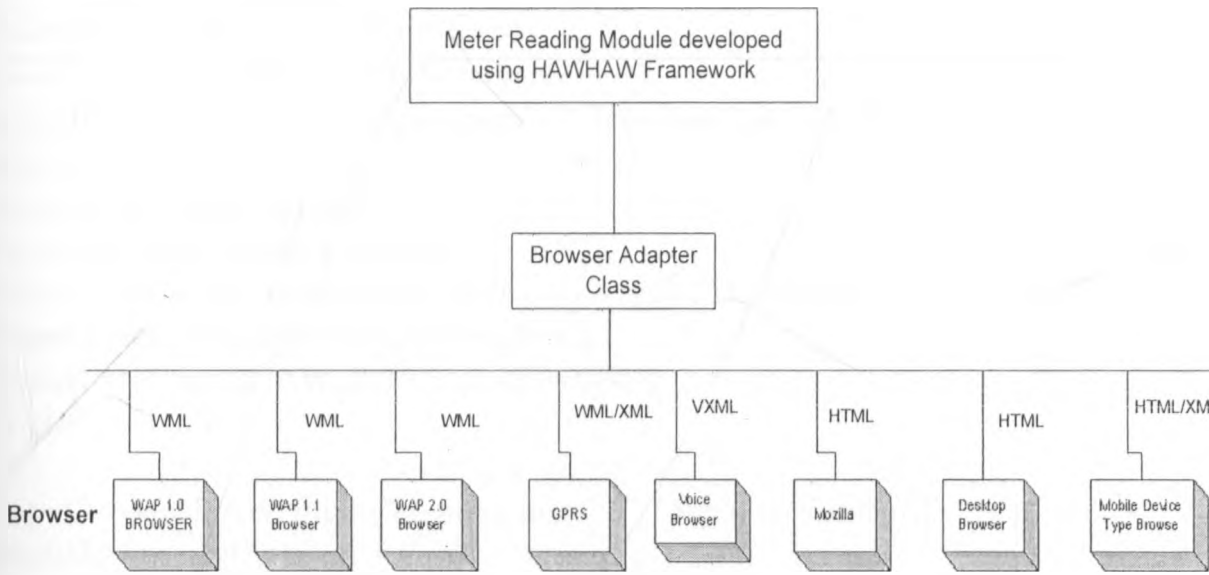


Figure 3.7 Device Adapter Module Functional Representation

4.4.2 Meter Reading Module

The meter module is made up of the authentication module which is a two way approach and two main modules Meter reading module and meter processing module. Authentication script receives the user credential from the SMS gateway and establishes a session ID then pushes the URL with encoded session ID using md5 encryption algorithm to the user.

The user will access the page which will pass through the gateway then to the device adapter module to detect the browser and render the form accordingly. The meter module is developed using the HAWHAW framework to offer adaptability. Below is a snippet of the meter reading module

```
<?php
```

```

// Include class to generate output
require('hawhaw.inc'); //the hawhaw framework implementation libraries.

// Create page and use simulator to test and debug
$page = new HAW_deck("Submit Your Meter Reading");
$page->use_simulator();

// Set application root for VoiceXML output
$page->set_application("appvoice.vxml");

// Create a new form to enter a meter reading
$form = new HAW_form("meter_Submit.php");
// Create a submit button for the form
$submit = new HAW_submit("Submit");
$input1 = new HAW_input("pin_num", "", "Pin Number:", "*N");
$input1->set_size(4);
$input1->set_maxlength(4);
//voice for voice browser enabled
$input1->set_voice_text("Please enter your 4 digit PIN number.");
$input1->set_voice_type("digits?length=4");
$input1->set_type(HAW_INPUT_PASSWORD);
$input1->set_br(1);

$input2 = new HAW_input("account_num", "", "Account Number:", "*N");
$input2->set_size(7);
$input2->set_maxlength(7);
$input2->set_voice_text("Please enter your 7 digit account number.");
$input2->set_voice_type("digits?length=7");
$input2->set_br(1);

$input3 = new HAW_input("reading", "", "Meter Reading:", "*N");
$input3->set_size(8);
$input3->set_maxlength(8);
$input3->set_voice_text("Please enter your 8 digit meter reading.");
$input3->set_voice_type("digits?length=8");
$input3->set_br(1);

// Add input items and submit button to form
$form->add_input($input1);
$form->add_input($input2);

```

```
$form->add_input($input3);  
$form->add_submit($submit);
```

```
// Add form to page  
$page->add_form($form);  
// Render the page  
$page->create_page ();
```

```
?>
```

appvoice.vxml –This is used to welcome the meter reader incase he has a voice enabled browser. See appendix section appvoice.vxml implementation.

On submitting the data it's processed by meter reading processing function. Refer to appendix section for meter reading processing module implementation.

The module is developed in PHP using the HAWHAW framework to ensure adaptability and avoid using a different standard for internet applications and different standard for Wireless application.

To enhance security a two ways approach is used and session ID remains open for a short period of time and also session is only open for a user if he has been authorized to be in the field for that day. The figure below is the expected output Nokia 3110c.

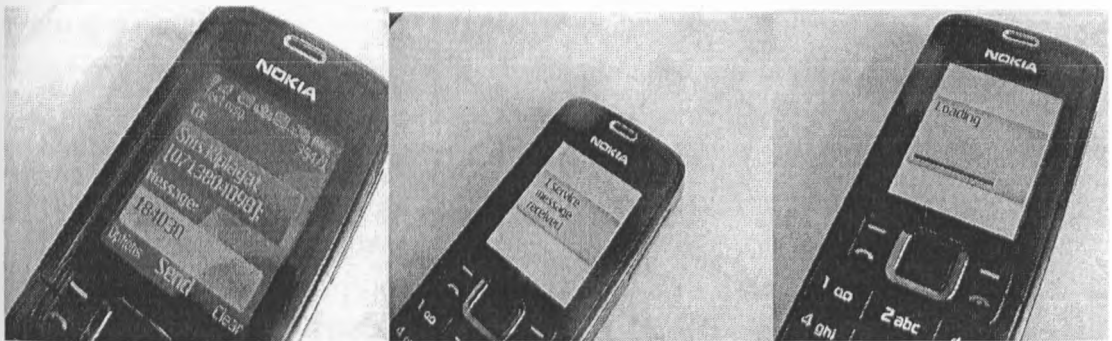




Figure 3.8 Meter Reading Module Prototype

4.4.3 SMS Messaging Module

SMS Messaging module was achieved through the configuration file. A file called `sqlbox.conf` was developed to handle SMS for inserting and retrieving from the database.

The SMS module is controlled by the `sqlbox` which is part of the `boxes` that are started when starting the `kannel`. It used to send and receive SMS. Refer to the appendix section for the configuration file for both `smsbox` and `sqlbox` which are configured and passed as parameter when starting the `kannel` as explained in the running the `kannel` section.

4.4.4 Emailing Module

We developed an emailing module in PHP that identifies the Emailing server and using SMTP protocol sends the attachment generated to the email of the customer retrieved from the database. The module will then delete the temporary file attachment from the file system of the server and saves a flag against the customer monthly statement to indicate that the statement has been posted to the customer. The module also checks the validity of the customer email to make sure that it actually exists to avoid sending statement to invalid email accounts. Below is a brief preview of the implementation function for the email module


```

function send_statement ($PdfFile,$CustID,$to_address,$to_name) {
//Company email details
    $from_address="dkiplagat@uonbi.ac.ke";
    $from_name="Nairobi Water Company";

    $reply_name=$from_name;
    $reply_address=$from_address;
    $reply_address=$from_address;
    $error_delivery_name=$from_name;
    $error_delivery_address=$from_address;
    $subject="Water Bill Statement";
    $email_message=new email_message_class;
    $email_message->SetEncodedEmailHeader("To",$to_address,$to_name);
    $email_message->SetEncodedEmailHeader("From",$from_address,$from_name);
    $email_message->SetEncodedEmailHeader("Reply-To",$reply_address,$reply_name);
    $email_message->SetHeader("Sender",$from_address);

/*
 * Set the Return-Path header to define the envelope sender address to which bounced messages are
 delivered.
 */
    if(defined("PHP_OS")
    && strcmp(substr(PHP_OS,0,3),"WIN"))
    $email_message->SetHeader("Return-Path",$error_delivery_address);

    $email_message->SetEncodedHeader("Subject",$subject);

/*
 * A message with attached files usually has a text message part
 * followed by one or more attached file parts.
 */
    $text_message="Hello ".strtok($to_name," ")."\n\n Attached is the Monthly Bill.\n\nThank
you,\n\n".$from_name";
    $email_message->AddQuotedPrintableTextPart($email_message->WrapText($text_message));
    $text_attachment=array(
        "Data"=>"This is just a plain text attachment file named attachment.txt ",
        "Name"=>"attachment.txt",
        "Content-Type"=>"automatic/name",
        "Disposition"=>"attachment"
    );
    /* attaching a text file commented
    //$email_message->AddFilePart($text_attachment);
    $image_attachment=array(
        "FileName"=>"http://10.2.22.196/websmis/dompdf/www/$PdfFile",
        "Content-Type"=>"automatic/name",
        "Disposition"=>"attachment"
    );
    $email_message->AddFilePart($image_attachment);

/*
 * The message is now ready to be assembled and sent.
 */
//call the send email function
    $error = $email_message->Send();

```

4.4.5 PDF Generator Module

We developed a PDF generator module in PHP that identifies the retrieves the customer's records and format it has a well formed html string. The HTML string is then passed as a variable to the PDF generator module which converts the HTML string into a PDF file and stores it in a temporary file for the Email module to class to attach. Below is a brief preview of the implementation function for the PDF generator module

```
function PDF_Generator ($CustID) {  
  
    //retrieve html string of the customer monthly bill  
    $html = html_string($CustID);  
    $CustID_real=$ CustID;  
    $CustID =str_replace("/", "_",$CustID);  
    $regno="./".$ CustID.".pdf";  
    $PdfFile = fopen($CustID,'w');  
    $Mysql_Db = NewADoConnection('mysql');  
    $Mysql_Db->Connect('10.2.22.196','root','','ncc_water');  
    if ($html) {  
  
        if ( get_magic_quotes_gpc() )  
            $html = stripslashes($html);  
  
        $old_limit = ini_set("memory_limit", "100M");  
        //generate the PDF file using DOMPDF class  
        $dompdf = new DOMPDF();  
        $dompdf->load_html($html);  
        $dompdf->set_paper("a4", "portrait");  
        $dompdf->render();  
        $pdf = $dompdf->output();  
  
        // $dompdf->stream("dompdf_out.pdf");  
        fwrite($PdfFile,$pdf);  
        fclose($PdfFile);  
  
        //call the send function of the email function to send the PDF file  
        $result = send_statement($regno,$Regno_real,$emailto,$toname);  
        print $result;  
        exit(0);  
    }  
}
```

4.4.6 Administrative Module

To assist in simulating the prototype and general administration of the system a web based system was developed using PHP programming language. This include module to perform the following

- Mange employees

- Manage Customers
- Manage authentication
- Manage Sessions
- Monitor the system
- Manage mobile devices
- Access to the database records

4.5 Simulation and Evaluation of the Prototype

Three different simulators were used to simulate the system. The gateway and the web server were installed in one red hat Linux machine. The machine was configured as both as a gateway, Webserver and a database server. Another a computer was used as a simulator to run the three simulators (Nokia 7210 SDK, OpenWave and HAWHAW simulator). A real nokia 3110c phone was used to initiate the session and also acts as a customer phone for receiving notification. The same computer was used to access the customers' statement via email. Below are the diagrams showing the meter reading interfaces for the simulators.

Simulation of the prototype using Nokia 7210 SDK



Figure 3.9 Simulation Testing

4.6 USABILITY ANALYSIS

Overview

The usability of a system can be defined as the capability in human functional terms to be used easily and effectively by the specified range of users, given specified training and user support, to fulfill the specified range of tasks, with the specified range of environmental scenarios [25].

Usability analysis is a process of assessing the usability of products by some form of assessment, typically through observation of how representative users perform standard tasks using the product [25].

The high demand and fast growth of mobile applications have attracted extensive research interests. Because developing mobile applications with an easy-to-use interface is critical for successful adoption and use of applications, one of the important research issues is regarding how to conduct an appropriate usability test using mobile devices in a wireless environment. Usability testing is an evaluation method used to measure how well users can use a specific software system. It provides a third-party assessment of the ease with which end users view content or execute an application on a mobile device. An effective usability test has to be able to elicit feedback from users about whether they use an application without (or almost without) difficulty and how they like using the application, as well as evaluate levels of task performance achieved by users

There are various guidelines for usability testing of desktop applications. However, those established concepts, methodologies, and approaches commonly used in traditional human-computer interaction research are not always applicable to mobile applications [26] due to mobility and the distinct features of mobile devices and wireless networks. Ideally, usability testing of mobile applications should be carefully designed to cover all or most possible situations of a mobile environment [25]. In reality, however, this poses many challenges. For example, it is difficult to foresee the exact situations of the application use - users may be standing, walking, or sitting in a dark or bright environment while using an application. As a result, a usability test may have to concentrate only on certain aspects of a mobile application and sacrifice others. Furthermore, traditional research methodologies used in usability testing, including controlled laboratory experiments and field studies, have various limitations in a mobile environment, such as ignoring the mobile context or lack of sufficient procedural

control. Therefore, it is essential to develop guidelines for usability testing of mobile applications.

Because achieving a high level of user satisfaction is critical to the success of mobile applications, usability testing is a mandatory process to ensure that a mobile application is practical, effective, and easy to use, especially from a user's perspective.

Methodology used

To have a good measure of usability of the mobile product, the research was conducted by the intended users (Nairobi Water Company). A questionnaire was prepared based on the usability framework defined in figure 4.4 below. To allow the users respond to the questionnaire the procedure for using the product was given and users tested the system. The test was also used to compute the average completion time of a transaction by logging in the start and end time of the transaction when the system is being used.

A framework for usability testing of mobile data collection system

This research presents a new framework for usability testing based on a typical human information processing. It defines the usability as the degree to which the users are satisfied with the product with respect to both the performance and the image/impression. Usability is classified into four dimensions for testing: perception, learning/memorization, control/action and evaluative feeling [25]. The figure 4.3 below presents operational criteria for testing usability.

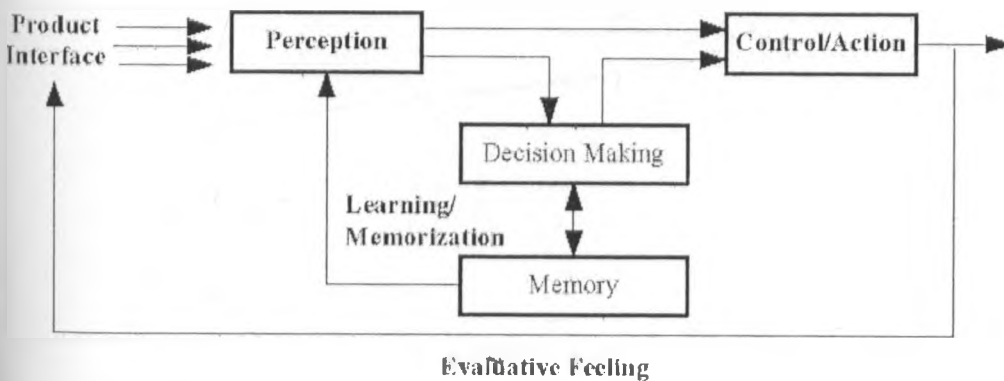


Figure 4.3 A human information processing of the product interface (adapted from [26, 27])

As illustrated in Figure 4.3, the performance dimensions, which stand for the specific criteria that should be used to evaluate the usability, were classified into

four categories: perception, learning/memorization, control/action and evaluative feeling. The classification was based on a typical human information processing [26].

- Perception: this category consists of the usability dimensions applicable to examine how well users perceive and interpret the interface of a product [27]. For the mobile data collection system, form size, visibility of the form is examples of perception of the product interface.
- Control/Action: this category represents the dimensions that explain the users' control activity and its results [27]. Speed of form entry, Simplicity, comprehensibility, Reliability, data capture, Efficiency, Responsiveness, rectification of errors is examples of the control/action on the system.
- Learning/Memorization: this category explains how fast the users get used to the product and how well they remember it [27]. Guidance capability, predictability, Memorability, consistency, informativeness and responsiveness are the typical factors of this category.
- Evaluative Feeling: this category is supposed to explain the attitude or judgmental feeling about a product [27]. Comfort, logic, attractiveness, satisfaction, acceptance, usefulness and convenience are the typical factors of this category.

Based on the four dimensions of usability, the criteria for usability testing are defined for mobile data collection system. The framework of usability testing of the mobile data collection system is constructed in Figure 4.4.

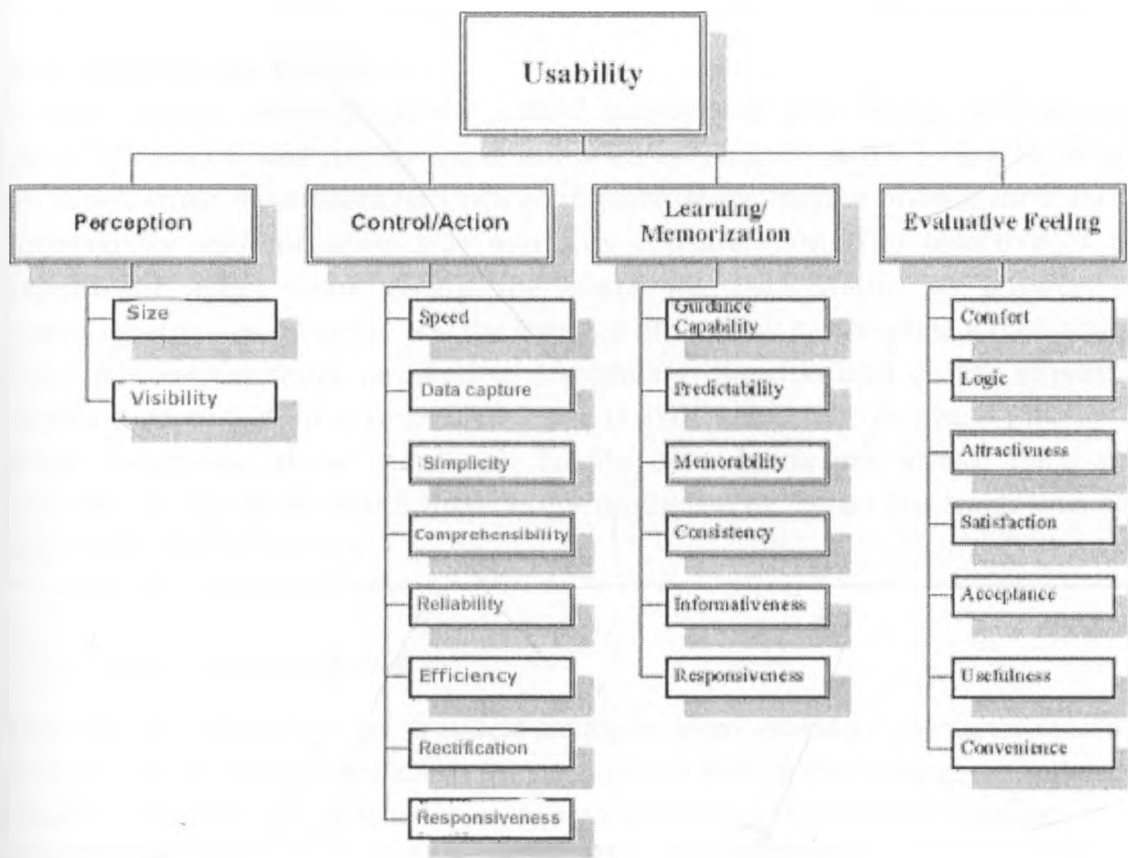


Figure 4.4 a framework for usability testing of data collection system

As illustrated in Figure 4.4 the usability of data collection system can be tested according to four dimensions: perception, learning/memorization, control/action and evaluative feeling. For each dimension, the operational criteria for testing are illustrated.

Usability testing of mobile data collection system

Using the framework in figure 4.4 above, usability analysis was done based on the framework. The research questions were identified and constructed based on figure 4.4 above. For the research to be effective we approached one of the utilities companies the NWC to use there human resources which they accepted. Attached in Appendix E is the procedure for testing and usability questionnaire the users were given.

EXPERIMENTAL DESIGN

In this usability research project a field survey was done using real intended users. The server was configured to allow access globally and a Nokia 3110c was provided since most users had not configured their mobile phones for internet connectivity and for some was monetary consideration. The objective of the experiment apart from giving the users the background to answer the questionnaire was meant to test the average time taken to complete a transaction. After the test the tester is asked to complete a questionnaire on the survey of mobile data collection system. The tester is allowed to take as much time as he needs to answer those questions. Totally 34 subjects are tested. Each was expected to repeat the test 5 times but a minimum of 2 tests per tester was also within the accepted range.

○ *Data Collection Method*

Task test is conducted so as to collect firsthand from intended user environment data and understand more about the usability of mobile data collection system. Coupled with the task test, a survey is also conducted. The targeted survey quantitatively addresses findings of the usability of the system.

○ *Test Process Design*

In this research, every participant is asked to perform the test 5 times but 2 times is also accepted. The system logs the start and end time of the transaction. The tester is asked to complete the task at a pace that feels natural to him. The tasks are designed as follow list:

- 1) Using a registered mobile phone with WAP connectivity send a message with your User ID provided to **0713-804-098** to establish the session, get the system address and provide a 2 way authentication channel.
- 2) A service message will be send to the mobile phone. Click on OK Key to browser the site provided
- 3) A form for meter reading will be provided. Fill it with the account number, the PIN and the meter reading and click on the submit button to post the reading.
- 4) If successful. A message indicating success will be displayed and a link to read the next meter will be provided
- 5) When through with the tasks check customer_nwc@uonbi.ac.ke to retrieve

and download the bill statement.

The actual procedure is provided in appendix E.

- *Questionnaire Design*

The questionnaire is titled "Survey on the usability of data collection system". A total of 22 questions were surveyed, including 2 questions concerned on perception, 8 questions concerned on control/action, 6 questions concerned on learning/memorization, and 6 questions concerned on evaluative feeling. Besides, some questions about subjects' background are designed, which could help to describe the sample characteristics. The survey used a 5-point Likert scale where. 1=strongly disagree, 2=Disagree, 3=neither agree nor disagree, 4=Agree, 5=strongly agree. The questionnaire is attached as appendix E.

- *Targeted Respondents*

In this study, the targeted sampling was focused on obtaining a high quality sample of real meter readers and their supervisors. Most interviewees are 31-40 years old and all respondents had used mobile phone for a period of two to eleven years. This sampling is considered a well-defined population selection with relatively high quality and stringency. To further minimize sampling errors, each individual solicited for a response was requested to provide accurate and well thought out responses.

RESULTS

- *Test Findings and Analysis*

- 1) *Transaction Completion Time*

The raw logs is for determining the completion time of each transaction is attached in appendix E. the table 1.3 below shows the average completion time of each participant.

#	Participant Code	No. of Transitions	AVG (seconds)
1	184030	8	159.00
2	184031	14	160.29
3	184032	4	164.50
4	184033	6	143.33
5	184034	5	187.00
6	184035	6	146.33
7	184036	2	184.00
8	184037	2	118.00
9	184038	2	113.50
10	184039	2	206.50
11	184040	2	172.00
12	184041	2	99.00
13	184042	2	97.50
14	184043	2	94.50
15	184044	2	89.00
16	184045	2	98.50
17	184046	3	147.67
18	184047	3	150.33
19	184048	2	139.00
20	184049	3	176.00
21	184050	2	206.00
22	184051	2	99.00
23	184052	2	102.50
24	184053	2	82.50
25	184054	2	84.50
26	184055	8	149.63
28	184057	5	369.40
30	184059	4	127.50
31	184060	25	102.00
33	184062	5	86.60
34	184063	5	351.20
GRAND AVG TIME TAKEN		136	150.99

Table 1.3 the average completion time in seconds taken by each participant.

From table 1.3 above a line graph analysis was done to show the trend of the average completion time shown in figure 4.5 below.

Average time taken to complete a transaction

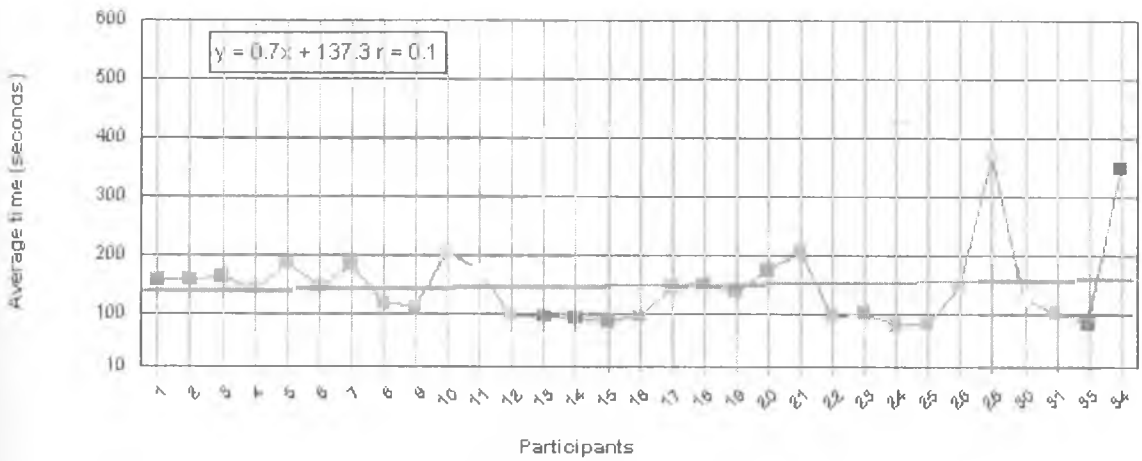


Figure 4.5 Average time taken to complete a transaction

It can be seen from the graph the average completion time of each transaction is 151 seconds. That is from the time of authentication initiation to posting of email to the customers email account. Most participants took around 150 seconds to complete the transaction which translates to three minutes to complete the transaction. Compared to the manual process taking an average of one month and logger process which takes 15 days, the mobile data collection and customer information system will actually achieve great results within the shortest time possible. It's important to note that the completion time can be affected by the speed of the user, the type of phone being used and the reliability of the mobile network. However in all cases the time taken will not be more than 10 minutes the time we had indicated in this research to achieve. This can be shown very well from the research where the experiment was performed for a period of three weeks and the highest completion time recorded was about 360 seconds translating to 6 minutes hence our hypothesis is true.

In conducting the usability test, testers faced various challenges which included lack of WAP enabled phones provided by the utility providers or interviewer due to budget constraint. We were forced to provide one mobile phone which was controlled by the billing officer. She will always call the meter readers at there convenience to perform the test which took unnecessary long time to finish the research.

Secondly, Most of the participants had not browsed using a mobile phone before and some had difficulty typing in numbers since the prototype had not been

validated to accept only numbers.

Few participants made general comments; however for those who took time to comment they recommended the following should be done

- The mode of keying in entries should be improved
- The cursor should automatically move to the next object on pressing OK key
- Authentication should be done once at the beginning of the day to save credit. If possible this should be done centrally at the server when the meter reader is being assigned the days work.
- The mobile meter reading should replace the logger immediately.
- On authentication allow a user to post as many transactions for that day until he signs off without the necessity to authenticate for every meter reading.
- The user form color should be modified and the form text area enlarged.

Most of these comments especially authentication should be considered when rolling out the product for market use.

2) Results of the Survey

The analysis of the survey data was based entirely on usable samples. Final results were read into a computer using Microsoft Excel and then transferred into access database for analysis using crystal reports 9.2. The means and standard deviations of all variables are summarized in Table 1.4. Refer to appendix E for complete raw data for this survey.

Dimension	Question No.	Attributes	N	Mean	STDEV
Perception	1	size	34	4.08824	0.93315
	2	visibility	34	4.26471	0.82788
Control/Action	3	Speed	34	4.42424	0.70844
	4	Simplicity	34	4.29412	0.75996
	5	comprehensibility	34	4.26471	0.79043
	6	Reliability	34	4.02941	0.90404
	7	data capture	34	4.08824	0.86577
	8	Efficiency	34	4.05882	1.01328
	9	Responsiveness	34	4.08824	1.05508
	10	Rectification	34	3.79412	1.09488
Learning/Memorization	11	Guidance Capability	34	4.00000	0.92113
	12	predictability	34	3.76471	0.95533

	13	Memorability	34	4.23529	0.78079
	14	consistency	34	4.06061	0.86384
	15	Informativeness	34	3.94118	0.95159
	16	Responsiveness	34	3.91176	1.21525
Evaluative Feeling	17	Comfort	34	4.11765	0.76929
	18	Logic	34	3.97059	0.83431
	19	Attractiveness	34	3.97059	0.90404
	20	Satisfaction	34	4.26471	0.93124
	21	Acceptance	34	4.11765	0.91336
	22	Convenience	34	4.41176	0.82085

Table 1.4 the means and standard deviations of all variables

In order to ascertain that the items listed in different dimensions do “hang together as a set”, a reliability test based on Cronbach’s Alpha test is performed using SPSS Refer appendix E.

The results are summarized in Table 1.5.

Dimension	Cronbachs Alpha (reliability Test)
Perception	0.8558
Control/Action	0.7082
Learning/Memorization	0.7682
Evaluative Feeling	0.8290
Overall	0.8434

Table 1.5 cronbach’s alpha test of different dimensions

Reliability coefficient of more than 0.6 is generally considered to be acceptable. The closer the reliability coefficient gets to 1.0, the tighter correlation among the factors in one dimension. The results shows that questions in all four dimensions do reliably hang together as a set, i.e., questions are properly defined into different dimensions. The Cronbach’s Alpha value of all the questions is also greater than 0.6 in all cases, i.e., questions is properly defined for the usability testing.

Line Graph showing comparison of means of all variables is illustrated in figure 4.6 below

Comparison of mean and standard deviation of all variables

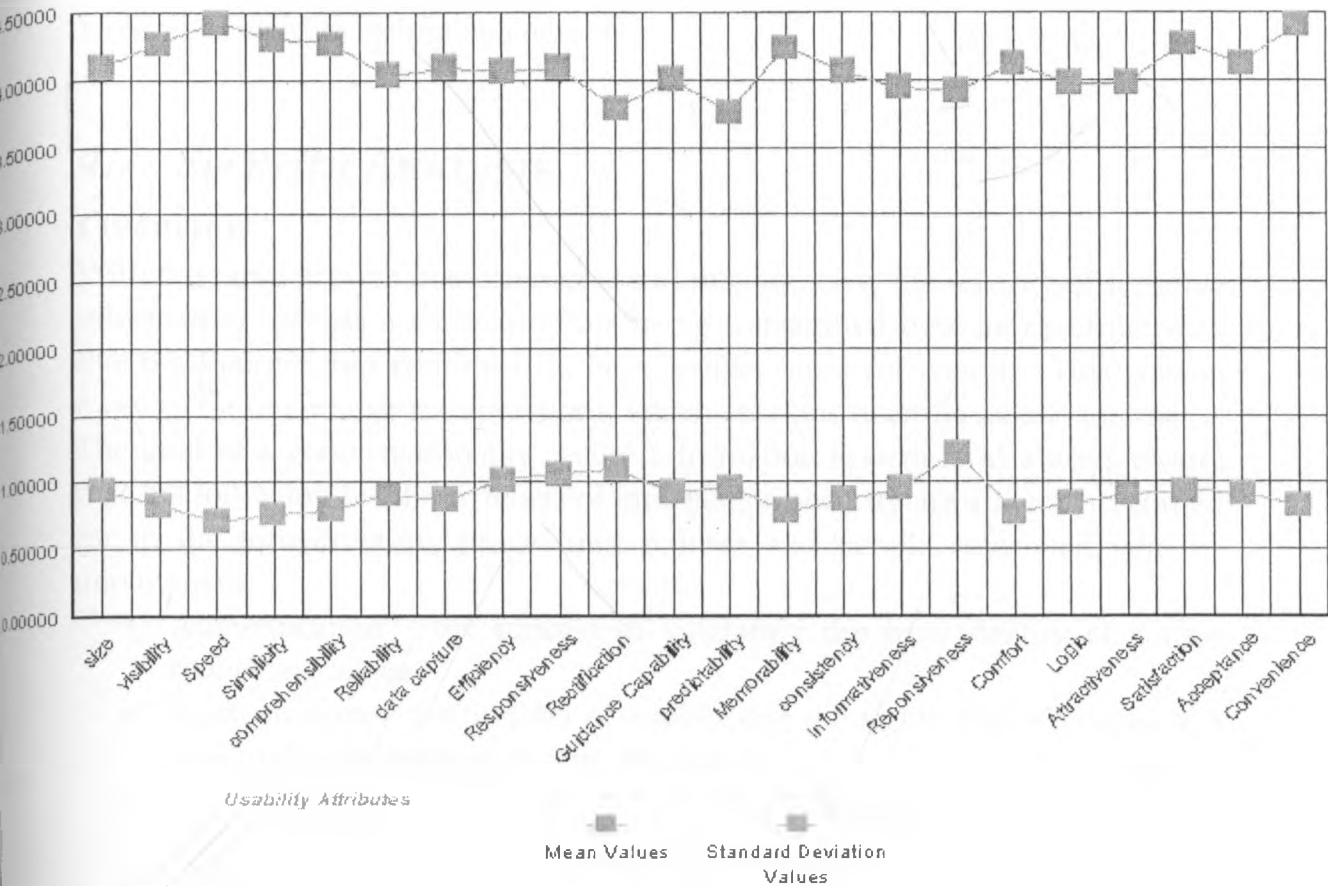


Figure 4.6 Graph showing comparison of means and standard deviation of all variables

Figure 4.6 shows that respondent's present positive response on most criteria of the mobile data collection system. Furthermore, respondents show similar response on most criteria of the system, which can also validate the classification of the four dimensions and the definitions of the 22 criteria for usability testing. The results also show that most respondents prefer the mobile data collection system hence resistance will be minimal, this can be attributed to the fact that the meter readers are assured of their jobs. Most respondents seem not to be comfortable with the authentication method and data entry procedures this is expected because there is always a thread of between security and usability otherwise its important to improve the data entry method including voice recognition which has been incorporated into the system. Otherwise all the

respondents were very excited about the possibility of such a system and are looking forward to its implementation.

4.7 Security Analysis

Overview

With the rapid growth in e-commerce and m-commerce, the security of sensitive information such as a corporate data being transmitted over an open network like the Internet, has continued to be a serious cause for concern. This is even more so for m-commerce transactions, which are done over the mobile Internet. The goal of a good, reasonably secure information system is to always ensure that the following five basic tenets of information security are all well accounted for in the infrastructure, procedures, policies and people associated with its deployment:

- Authentication – the process of validating the true identity of a user requesting access.
- Authorization – the method of establishing the rights and privileges of a user during its interaction with the system.
- Confidentiality – the means of ensuring that all sensitive data being transmitted can only be read by authorized parties.
- Integrity – the process of preventing alteration of data in transit by unauthorized third parties.
- Non-repudiation – the means of proving the occurrence of a transaction and making it impossible for parties involved to deny carrying out the transaction.

Wireless security is in many occasions comparable with the security of its wired equivalent. But still the mobility and increasing amount of wireless devices and networks bring new threats and make many of the old ones even bigger.

Wireless security has lots in common with security in fixed networks as the basic rules for the both are the same – same basic tools can be used in both but many of them are more crucial to implement in the wireless world to maintain the same level of security. Wireless communications have some specific characteristics over the fixed communications that have to be considered in the sense of security.

Those are:

- Transmission through air: anyone can listen (privacy)
- Radio waves do not stop to corporate walls or to other artificial borders (privacy)
- Spectrum of the radio channels is limited (availability)
- Without network coverage no services available (availability)

Keeping data private is a big issue for any wireless network. In the days of voice-only communications, the greatest worry was that an eavesdropper could listen to a private conversation, but mobile commerce makes security even more critical – if people are going to entrust their bank account to technology, it has to be secure.

Security is an important enabler for the development, adoption and the usage of the mobile and wireless technologies and services. Business, as well as consumer, applications will not be able to realize their fullest potential unless a sufficient level of trust is established in the underlying security of mobile networks.

4.7.1 Security threats

The same basic security threats are confronted in fixed and wireless networks, but the wireless and mobility brings a new aspect for all of them. Due to the high and ever increasing number of wireless and mobile devices the affects can be exponential to those of the fixed ones.

The basic types and threats are:

- Attacks

- Intellectual property theft
- Identity theft
- Brand theft
- Destruction of data and/or equipment

-Privacy violations

- Surveillance
- Databases collecting private information -traffic analysis
- Massive electronic surveillance

-Publicity attacks

- Disturbance or interception of communication
- Denial-of-service (DOS) attacks

4.7.2 Security Analysis of mobile data collection system

The basic module of mobile data collection is implemented through WAP model discussed earlier. WAP has two major undoing that this research project as dealt with and which has lead to the poor adoption of WAP as a model for mobile internet.

- Lack of end to end security on change from WTLS to TLS or SSL.
- Failure to utilize the standard HTML such that programmers have to develop pages for the internet and separately those of WAP using WML standard.

The lack of end to end security has already been explained and solution offered and failure to utilize standard HTML has been dealt with by using HAHAW framework to come up with a development framework that is device and browser independent. In this system the entire framework was split and five categories identified as a point of security thread these are;

- Device security
- Network security
- Gateway security
- IP security
- Server security

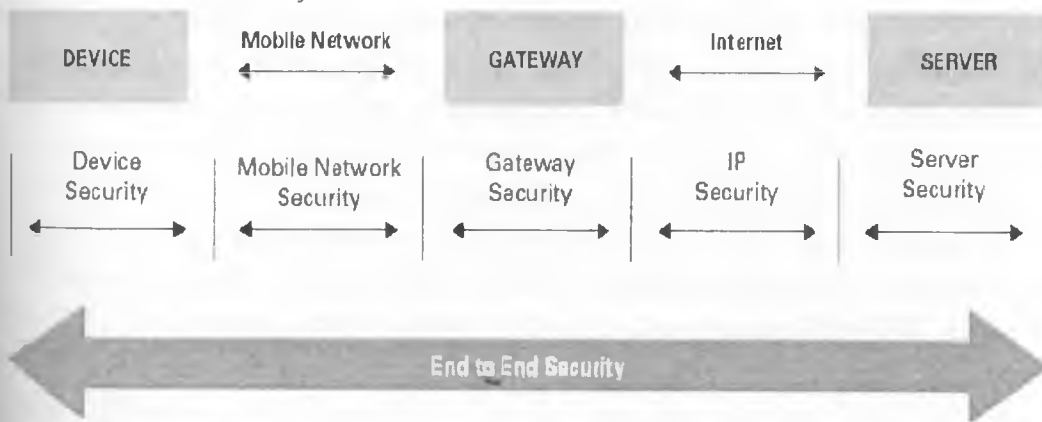


Figure 4.7 Model security analysis

Device security

Mobile devices are commonly the weakest link today in the converged data

world. The diversity of standards available and their relative immaturity makes it very difficult to impose sufficient security standards on mobile device access. The importance of the device security comes into spotlight in corporate adoption of the devices as they are becoming business tools to be used with corporate IT-infrastructure: even a robust and expensive security infrastructure may be easily penetrated through a mobile device security hole.

From devices point-of-view there are features to point out that are generally causing security problems. These are:

- As they are wireless and mobile, they can be taken almost anywhere, not just in locked corporate premises -Typically they are small and light making them easy to lose or steal
- As the amounts of the devices is rising they are becoming a more attractive target for attackers
- Hardware features set the limitations for certain security software to be used on the device itself (CPU, memory, battery life, etc.)
- Since Request of session ID and URL is done through SMS. SMS is very insecure and someone can pretend and send SMS claiming that you are the originator. Since SMS is stored on the SMSC and mobile phone the message can also be altered

Solution

In this model the security of the device has been secured by using two way authentications to make sure that the device being used is from the authorized person. The meter reader sends a message with his credential which theoretically is known by the meter reader only. The system checks the credential send and the mobile number of the user. Assuming someone send the right credential and manages to forge the mobile number user, the system will push the URL and session ID for access to the system. The user will be required to enter the PIN which is generated whenever a meter reader is to go to the field through the corporate intranet system. So the imitator will face the second handle of guessing the PIN. Assuming going against all odds he guesses the PIN right then on posting the details of which the meter reading should be above the previous, the WAP gateway will pass the WAP header file to RADIUS server for authentication and if the registered user MSISDN is not the same as the claiming user MSISDN the security system will be informed and the account locked. So the hacker cannot use other device other than the registered user device. Authorization can further be enhanced by Wireless Identity Module (WIM). WAP devices can use a Wireless Identity Module (WIM) which contains the

necessary private and public keys to perform digital signatures and certificate verification respectively. It is a tamper-proof device, which means that it is very difficult for an attacker to obtain the keys which are stored in this device. The WIM can be compared to the SIM of the GSM or smart card authentication mechanism.

Network security

Wireless communications use air interface to carry the electromagnetic waves that carry the information. The air interface has the security concern that anyone in the range of the communication can intercept the data being transferred through it. And it is a lot easier than intercepting communications in fixed network as the waves in the air go all over but in the fixed line they do not leak out of the cables; in the fixed world the eavesdropper has to know where the lines are going to tap to them.

Other security problem with the air interface has been the fact that the radio waves will not stop to certain borders like organization's physical premises. This is serious problem with WLAN implementations as in the cities many offices are building their own WLAN networks near to each other as one might think the possible concerns in a office building where in every floor resides a different company with its own and different WLAN. This is basically equivalent to leaving an open network connection for everybody to peruse without the need to physically plug in a cable. To a certain degree, this issue is addressed by a standard security function called Wired Equivalent Privacy (WEP). In many cases this technology alone is not sufficient, so additional security options are being developed for WLANs to enhance the protection provided by WEP.

For data security reasons almost all wireless networks have to have some degree of network security with their own security (encrypting) algorithms or mechanisms. The degree of the security within the network without outside encrypting depends on the network. For example, GSM communication is encoded with a 128k algorithm to ensure secure wireless transport. Each of the users is assigned a temporary code that enables them to receive only the digital signal sent to them. In an eavesdropping scenario the time required to crack the code is usually longer than the life of the temporary key. The security offering capability of the upcoming UMTS system is going to be higher due to the higher data rates and more complex modulation schemes. Alternative network technologies are to a larger extent subject to security issues.

Solution

In wireless network security is provided by the WTLS layer of the WAP protocol

and the wired network or the internet by TLS or SSL. The WAP gap between the two protocols is solved by hosting the WAP gateway within the corporate wired network and having the RADIUS server acting as authentication server for remote users. Another solution is which administrators can consider later is the establishment of Virtual Private Network (VPN) connects computers and devices, which can be located around the globe, to a private network using public networks. A VPN is a 'virtual network' since connections are established only on a when-needed basis. The transmitted information is encrypted and tunneled point-to-point over a packet-switched insecure network. At the receiving end, the information is decrypted, filtered if necessary, and checked for integrity. A VPN provides network users with an inexpensive, safe and scalable security solution. VPN can be implemented in several ways and in different levels. It can be implemented between two local area networks (LAN-to-LAN), from remote user to local area network or within an intranet [19].

Figure 4.8 illustrates a virtual private network connection from mobile device

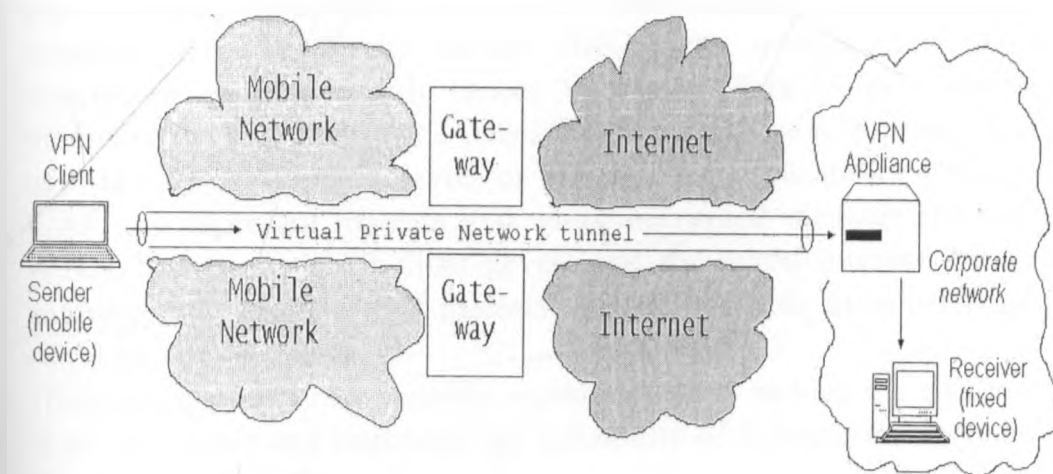


Figure 4.8 VPN Network (adapted from [19])

Gateway security

Gateways operate between the mobile or wireless devices and the fixed network providing the information of fixed network to the device and vice versa. In some cases the gateway also transforms the content to a form that the other end can understand it. On a higher level, communication between the device and the

gateway is also subject to being protected by data security protocols. The transforming of the information from another encrypted form to another is then done at the gateway. In the former version of WAP (1.1) this was done by first decrypting the content and then encrypting it again with the other algorithm. This left a little theoretical time space open for hackers to get the content in plaintext. In the newer release of WAP (2.0) this should have been addressed.

Considering that wireless networks are generally more vulnerable than wired networks, a number of wireless security standards have been developed to ensure the security of information transmitted over the wireless Internet. For instance, Wireless Application Protocol (WAP) solutions use the wireless transport layer security (WTLS) in place of Secure Socket Layer (SSL) or Transport Layer Security (TLS) to ensure secure transmissions between WAP client devices and the WAP gateway. However, communication between the WAP gateway and the backend application or Web server is over a wired network and thus uses standard TCP/IP based Internet security protocol such as TLS or SSL. This scenario therefore creates a need for inter-protocol translation to be handled within the WAP gateway. This results in what is known as the “WAP gap” (Security loop Hole), which is a subtle security issue within WAP-based solutions. The WAP gap occurs due to the inter-protocol translation or conversion process, which causes encrypted data to be decrypted, albeit momentarily, and then re-encrypted before transmission from the WAP gateway to either the WAP client device or the backend application or Web server. The WAP gap represent the fact that every encrypted message transmitted using WTLS, between a WAP client device and the wired Internet through a WAP gateway, will at some brief instance exist as readable plaintext whose security could be compromised.

There are a number of possible workarounds to reduce the risk posed by the WAP gap issue and minimize the possibility of it being maliciously exploited. These include:

- Ensuring the WAP gateways at the wireless network operator’s premises are installed within a heavily secured data centre area with very restricted access. The best practice is to install the WAP Gateway at the application server or the web server. Avoid outsourcing the WAP gateway for critical application.
- Designing the message translation process handled within the gateway such that all encryption, decryption and encoding take place within memory without the use of any temp files or explicit writes to disk.
- Ensuring that no details of the translation are ever logged to disk.

- Hosting the WAP gateway within the same secured wired network (i.e. wireless application owner's own network) as the application server and taking full responsibility for its administration. This ensures that all the inter-protocol translation process is done within the wireless application owner's secured network.
- Use of RADIUS server between the WAP gateway and the Wireless provider.

Server security

Server security is not directly related to the mobile security but servers are in an important position for the services and applications and very important components of an end-to-end mobile data security infrastructure. Servers might store valuable and confidential information that is not meant to be open for public. Only the individuals with permission have to be let in to access that information. Also the availability of services should be guaranteed. With increasing numbers of mobile devices hackers will be attracted to try to exploit the possibilities of doing so called denial-of-service attack, laming down a server with too many requests from millions of devices that they possibly could gain the access. Also the servers are in a key position to spread malicious code to other devices or to prevent it.

Solution:

Authentication

Authentication is about the continuity of relationships, knowing who to trust and who not to trust, making sense of a complex world. People authenticate themselves many times a day, even without recognizing it, but it is still one important part of our daily lives; recognizing the faces, voices or other recognizable features of our trusted partners, colleagues, relatives or even goods or services.

In this project we implemented a two way approach to authentication as explained earlier. Also only the meter reading interface is available over the WAP. The administrative module is done within a web based interface within the corporate network

Firewall

Firewalls have generally been used to separate corporate intranets from the Internet by providing access control. A properly configured firewall prevents unauthorized access to or from private networks, especially Intranets. All messages (i.e. all IP traffic) entering or leaving the Intranet pass through the firewall, which examines each message and blocks messages that do not meet the specified security criteria. A Firewall is one of the fundamental components of a secure network.

Firewalls can be hardware or software based. Hardware based solutions are often designed for large scale IP traffic such as large corporation intranets. Software based firewalls are designed for smaller IP traffic, such as even single computers. In the age of powerful viruses and worms and always-on connectivity it is also recommendable to have a software based firewall on a single computer to prevent unauthorized access and usage

The Human Factor and Security Management

Computer security is difficult, to the vendors of software and hardware products, but also to the users of those products. Even if the hardware, the software and network were secure, the complete system could still be jeopardized by one user that does not care enough about security.

Security of computers and systems always interacts with users, and as commonly the user is a human, it is the security of the interaction between human and the computer or system. One does not need to look far to find an easy example of this. One such example would be a user that shares out confidential information like PIN with other people. Even though the system was secure, the user made the information insecure by carelessly handling it.

To reduce this incidence we recommend having a PIN generator that generates a unique PIN every time the user needs to go to the field

One important part of security management is the creation of company security guidelines. They are then the rules by which every employee must abide. The guidelines must also follow the rules according to which those guilty of breaking them are being punished. As important as the guidelines they are to inform and educate employees to obey them. When these steps have been taken it is the corporate responsibility to keep the infrastructure up to date.

Chapter 5: Discussion and Recommendation

5.1 Introduction

In order to provide suitable support in the context of less reliable networks suffering e.g. from lower throughput and higher latencies, the design of such system has to be reconsidered. Moreover, low-capable end devices pose additional requirements on sensible strategies for the development of such M-Solutions. Slow processors, a limited amount of memory, small displays, and low battery capacities have to be taken into account. Lastly, the cellular design of modern mobile networks shall be exploited. Besides their intrinsic scalability, cellular structures can simplify the integration of location-dependency considerably.

The Wireless Application Protocol as mobile counterpart of the ubiquitous and supposedly omnipotent World Wide Web is one the few middleware standards explicitly tailored for use in wireless environments on top of small end devices. The general idea behind WAP obviously is to continue the impressive success of the Web in the realm of mobile networks. However, the acceptance of WAP is still limited—not without reason.

This include the lack of end to end security between wireless to wired which in this research project we proposed the use of RADIUS server and using the kannel gateway which can be configured within the Webserver of the corporate network

Secondly, need for content providers to develop two completely independent and diverse versions of their Web pages. Although the limitations imposed by mobile stations and WML browsers require a separate representation anyway, it is currently not possible to generate both versions out of a common base document due to considerable markup language diversities and to a minor degree lack of tool support. By implementing the device independent module within the Webserver and using the HAWHAW framework to develop application it eliminated this need to develop two completely independent applications for both wireless and internet.

5.2 Summary of research project

In this research project we began studying the various models of implementing mobile data collection system. We also identified the various challenges affecting the Utility providers and the current workflow. This was done by fact finding mission at NWC. Then taking into consideration the limitation of mobile devices, the challenges facing utility providers and the core objective of the research a hybrid model was developed.

The requirements as per the general limitation of mobile devices and the security required were analyzed and documented. Based on the requirements the design of the prototype was developed. Implementation was then done. Usability testing was done to ascertain the workability of the prototype within the real environment. Through testing and analysis of test results for structural correctness of the system was avoided since the objective was to develop a prototype and that is expected to be done by implementers in real environment. Based on the consideration to be done in real life both security and usability analysis was done.

5.3 Achievements

At the start of this research the following were the objectives if this research

- To carry out analysis of existing data collection models– Literature review was done on the existing mobile data collection models, there architecture, known shortcomings and advantages were investigated. From the analysis a model was developed by combining WAP, WWW,SMS addressing there shortcomings within the model to come up with a data collection model for mobile data collection.
- To identify data capture challenges facing utility providers – challenges facing utility providers were identified and shown how the proposed model will assist the companies to overcome them. Although not all challenges were exhaustively solved, the recommendation for further work if pursuit will be able to offer a comprehensive integrated secure mobile solution for utility companies to reengineer there metering services in terms of customer care and meter reading.
- To identify ways in which data capture, analysis and customer care workflow can be reorganized and made more efficient – current two main methods workflow of data collection was and areas that need business

process reengineering highlighted together with the savings associated with the flow. Then using the proposed solution, we proposed a new efficient workflow that will reduce human interaction and increase software module interaction such that only one person is involved in the entire process just to post the meter reading. This also achieved record security such that the originator actually takes the responsibility of the record entered through comprehensive audit trail.

- To identify cost effective ways in which hand-held devices can be used for data collection – after identifying the different models the WAP model was chosen after proposing the solution to their current limitation of WAP gap and adaptability. To be cost effective the model was then expanded to include other web services to enhance to customer information. These include the SMS solution, Emailing and PDF generator each performing a unique function in the model.
- To analyze security and vulnerability of the prototype and what enhancements can be done to make it more secure – Security analysis was done on the proposed model. The weakness identified and solution offered. This included the RADIUS implementation, hosting WAP gateway within the corporate network and implementing a two way channel of authentication, opening session ID when only necessary for a short period of time and PIN generation on the need be basis.
- To develop a working prototype of the system based on the proposed model, - The prototype was implemented using purely open source products. All the main modules were implemented and tested to make sure they are working within the expected time limit.
- To evaluate the usability of the system in view of the limitation of the mobile devices– The usability of prototype was tested to test workability both in terms of proposed structure and time taken to complete a transaction. Features to make the system more usable were implemented including reducing number of clicks to one, pushing URL instead of typing and validating data entry to ensure that fields for numbers accept only numbers and length etc. Adaptability was included using the device independent framework and coding based on one standard for all the

devices. We were able to perform usability test and survey research with real intended users courtesy of NWC.

5.4 Limitations and Challenges

Limitations

In the process of developing this research project, quite a number of challenges and limitation came up along the way. Some of these changes were;

- The number of servers required. From the model at least three servers were required. That is for Gateway, Webserver, and RADIUS and database server. All this were combined to one physical server which might affect the behavior of the system in real environment in terms of speed.
- Lack of different models of mobile phones to give to the participants to test the system.
- Real environment testing had a costing implication for airtime and data transmission hence limitation of test to very few test runs.

Challenges

Configuration of the Kannel WAP and SMS gateway proved a taunting task because of poor documentation and support.

Development of the configuration file for the USB Samba Edge modem proved a monumental task because it was a new device in the market and I had to get the technical manual from the supplier after struggling with it for more than one month.

Another challenge was testing the voice component of the meter reading module because of lack of voice browsers and most simulators available require payment to host the site testing.

Another challenge was given that WAP technology is a fairly new research area material available are not adequate and sometimes contradictory depending on the biasness of the author.

Lastly, integration of all the technologies used in this research proved a daunting task. But we managed in the long last to develop all the modules anticipated and tested their workability. Also lack of funds to get every device required was another handicap.

5.5 Suggested further research:

Mobile technology and in particular m-commerce is still a new field of immense research currently. So far all indication is that with the introduction of gigabit network the 3G the m-commerce will by pass the e-commerce which is yet to gain strong foothold. The sheer number of mobile users alone makes it a very interesting area to role out customer targeted specific services. In the area of meter reading services the challenges facing utility providers are many and this research although it tried to sort out quite a number of them there were some specific that were not within the scope of this project due to time constraint and need to have others contribute to this interesting field. Two particular challenges facing utility providers require further research and work this are

- Ensuring that the meter readers actually visits the site and gets the correct values
- Visiting of customer premises which they might not allow or have some dogs that can cause harm to staff reading the meters.
- Efficient and convenient customer payment systems

The first one of ensuring meter readers actually visit the site and get correct values, although in this research the fact that customer will immediately via SMS or GPRS message get a confirmation message of the current meter reading which he can immediately confirm with the meter reader and take appropriate action will assist, it is not a water tight method because the owner might be disinterested to confirm or at the work place when the meter is being read. The best method is to implement a two way approach. That is integration to Geographical Positioning system via GPRS and integration to a spatial database. Such that the locality coordinates of each meter is stored in the spatial database and when the meter reader is posting the readings the mobile phone also posts the coordinates where the meter reader is standing currently such that if it is not within the locality of the meter reading the posting are rejected on that basis.

Secondly the utility providers can barcode their meters with permanent code such that the system can be integrated with an imaging processing module. In this case before the meter reader authenticates to post the reading, using the

Lastly, integration of all the technologies used in this research proved a daunting task. But we managed in the long last to develop all the modules anticipated and tested there workability. Also lack of funds to get every device required was another handicap.

5.5 Suggested further research:

Mobile technology and in particular m-commerce is still a new field of immense research currently. So far all indication is that with the introduction of gigabit network the 3G the m-commerce will by pass the e-commerce which is yet to gain strong foot hold. The sheer number of mobile users alone makes it a very interesting area to role out customer targeted specific services. In the area of metering services the challenges facing utility providers are many and this research although it tried to sort out quite a number of them there were some specific that were not within the scope of this project due to time constraint and need to have others contribute to this interesting field. Two particular challenges facing utility providers require further research and work this are

- Ensuring that the meter readers actually visits the site and gets the correct values
- Visiting of customer premises which they might not allow or have some dogs that can cause harm to staff reading the meters.
- Efficient and convenient customer payment systems

The first one of ensuring meter readers actually visit the site and get correct values, although in this research the fact that customer will immediately via SMS or GPRS message get a confirmation message of the current meter reading which he can immediately confirm with the meter reader and take appropriate action will assist, it is not a water tight method because the owner might be disinterested to confirm or at the work place when the meter is being read. The best method is to implement a two way approach. That is integration to Geographical Positioning system via GPRS and integration to a spatial database. Such that the locality coordinates of each meter is stored in the spatial database and when the meter reader is posting the readings the mobile phone also posts the coordinates where the meter reader is standing currently such that if it is not within the locality of the meter reading the posting are rejected on that basis.

Secondly the utility providers can barcode there meters with permanent code such that the system can be integrated with an imaging processing module. In this case before the meter reader authenticates to post the reading, using the

camera takes the picture of the barcode which is sent to imaging module to decrypt and compare with the stored security code of the meter. This will also enhance on the security of the system.

Thirdly, further work should be done to investigate how to use mobile technology to avoid meter readers entering the compound of the customer while taking into consideration the cost of the solution to be proposed. Currently the viable option is imaging and Bluetooth technology which can be integrated to mobile devices which are Bluetooth enabled.

Lastly to complete a holistic solution m-payment system can be incorporated. In this case the system can be linked to MPESA solution or m-wallet for those with credit cards and debit cards such that when the customer receives a message of an email bill the customer using either the m-wallet or MPESA the can make the payment and the same system gateway will process the payment and post to the account number of the customer generate a receipt and attach it to email as a proof of payment for the customer to generate and file.

5.6 Conclusions

Utility providers will achieve a lot if they are to implement mobile solutions and e-technology to reengineer their metering services as shown by this research project. Wireless technologies bring many new possibilities for Utility providers to achieve flexibility and competitiveness or even make possible things that were earlier impossible to do. The main obstacle in utilization of wireless technologies will be the imagination, or more importantly, the lack of it. But as the new technologies may sound a little heaven on Earth, they can become a nightmare if certain things like security and the management of those technologies are not considered, planned and implemented well. Security measures have to be planned analyzed and executed with care to avoid loopholes which if it occurs might affect the role out of mobile applications. For sure, these new technologies will reshape the ways of doing work, business or services, maybe not all, but many of them. Mobile solutions will reduce the cost of doing business and reduce the number of processes required to complete a transactions thereby enhancing efficiency and effectiveness thereby increasing the return on investment and customer perception which is core to any business.

References:

1. Technical specifications and presentations by Scott Goldman
<http://www.wapforum.org>
2. "Nokia WAP Server 1.1 Security Pack", Nokia Mobile Phones
www.nokia.com/corporate/wap
3. "Ericsson Mobile Internet Enabling Proxy 1.0", Ericsson Radio Systems AB, www.ericsson.com
4. Product data sheet, Jinny WAP Gateway, www.jinny.ie
5. "WAP Gateway 3.0", Exomi Oy, www.exomi.com
6. "WAP 2.0 Technical White Paper", WAP Forum, www.wapforum.org, January 2002
7. Open Source Kannel Project, <http://www.kannel.org>.
8. Linux Virtual Server Project, <http://www.linuxvirtualserver.org>.
9. Php Classes Forum, <http://www.phpclasses.org>.
10. Damon Hougland, Khurram Zafar. 2001. *essential WAP FOR WEB PROFESSIONALS*. Upper Saddle River (NJ): Prentice Hall; 234 p.
11. Stallings, W. *Network Security Essentials Applications and Standards*, international second ed. Prentice Hall, 2003.
12. AU-System Radio AB. 1999. WAP White Paper. Available: <http://www.wapguide.com/> 28 February 2000.
13. Capone, J. (2002b): "*Addressing the Mobile application development and deployment challenge with Java 2 Enterprise Edition*." Accessed online at <http://www.aligo.com> on 16-Aug-2002.
14. Al-Saleh, A. (2001). "*Wireless Strategy: Guidelines for getting started*." *Wireless Business & Technology Magazine*. Accessed online at <http://www.sys-con.com/2001/wireless> on 18-August-2002.
15. HAWHAW Framework, project <http://www.hawhaw.org>.
16. Wikipedia, <http://en.wikipedia.org/wiki/Email>
17. Wei Meng, Soo Mee, Karli Watson, Ted Wugofski. 2000. *Beginning WAP, WML & WMLScript*. Birmigham (UK): Wrox Press; 650p
18. Niels Christian Juul and Niels Jorgensen
"Security Limitations in the WAP Architecture" Position Paper

19. Steve Lord, X-Force Security Assessment Services, and Internet: Trouble at the Telco When GSM goes bad. In *Network Security*, 2003(1):10 – 12, 2003
20. Margrave, D. GSM Security and Encryption. Available from: <http://www.hackcanada.com/blackcrawl/cell/gsm/gsm-sec/gsm-sec.html> (1999); accessed 27 October 2006.
21. Wagner, D. GSM Cloning. Smartcard Developer Association and ISAAC security research group. Available from: <http://www.isaac.cs.berkeley.edu/isaac/gsm.html> (1998); accessed 28 October 2006.
22. Burak Bayoglu: Performance evaluation of WTLS handshake protocol using RAS and elliptic curve cryptosystems, 2004.
23. Biryukov, A. Shamir, A. Wagner, D. Real Time Cryptanalysis of A5/1 on a PC. In *Fast Software Encryption Workshop*, 2000
24. Amit Vyas, Peter O'Grady, "A Review of Mobile Commerce Technologies", Department of Industrial Engineering, University of Iowa, May 2001
25. H. S.H., Y. M. H., K. J., and H. S.W., "Usability of consumer electronic products," *International Journal of Industrial Ergonomics*, vol. 28, pp. 143-151, 2001.
26. C. D. Wickens, S. E. Gordon, and Y. Liu, *An introduction to human factors engineering*. New York: Longman, 1998.
27. S. H. Han, M. H. Yun, J. Kwahk, and S. W. Hong, "Usability of consumer electronic products," *International Journal of Industrial Ergonomics*, vol. 28, pp. 143-151, 2001.

APPENDIX A: KANNEL CONFIGURATION FILES

Smskannel.conf configuration file for bearerbox and wapbox

```
group = core
admin-port = 13000
admin-password = sms
admin-deny-ip = "*"
admin-allow-ip = "127.0.0.1"
wapbox-port = 13002
wdp-interface-name = ""
log-file = "/var/log/kannel/bearerbox.log"
box-deny-ip = "*"
box-allow-ip = "127.0.0.1"
#smsbox-port = 13003
smsbox-port = 13001
#smsbox-port-ssl = yes
#unified-prefix = "+254,00254;+,00"
store-file = /var/spool/kannel/sms-store
dlr-storage = mysql
```

```
group = ppg
ppg-url = /cgi-bin/wap-push.cgi
ppg-port = 10080
trusted-pi = false
ppg-allow-ip = "*"

```

```
group = wap-push-user
wap-push-user = foo
ppg-username = foo
ppg-password = bar
```

```
group = wapbox
bearerbox-host = localhost
log-file = "/var/log/kannel/wapbox.log"
timer-freq = 10
#map-url = "http://localhost/* http://localhost:80/"
```

```
group = smsbox
#reply-requestfailed = "No existe un servicio asociado"
bearerbox-host = localhost
bearerbox-port = 13003
sendsms-port = 13013
log-file = "/var/log/kannel/smsbox.log"
access-log = "/var/log/kannel/kannel.access"
log-level = 0
global-sender = +254713084098
#http-request-retry = 3
#http-queue-delay = 15
#sendsms-chars = "0123456789 +-"
```

```
group = smsc
smc = at
modemtype = auto
# Choose appropriate one. I ended up with setting a symlink to the device, so I # do not need to change the config file
#every time the modem appears under# different device name.
device = /dev/ttyACM0
```

```

#device = /dev/mux1
#device = /dev/GSMSMS
#speed = 115200
speed = 460800
my-number = "+254713804098"
smc-id = "ES75"
#allowed-prefix = "0;+"
#unified-prefix = "+254,00254;+00"

# SMS modem Siemens ES75
group = modems
id = "ES75"
name = "Siemens ES75"
detect-string = "SIEMENS"
#detect-string2 = "MC75"
init-string = ATi+CSMS=1;E1;+CNMI=2,1,2,2,1
#keepalive-cmd = "AT+CBC;+CSQ"
#enable-hwbs = "AT\\Q3"
# line below required, otherwise sending fails
need-sleep = true
#message-storage = "ME"

# SMS service
group = sms-service
#keyword = default
keyword =
keyword-regex = .*
catch-all = true
#allowed-prefix = "0;+"
# Choose a method of passing the SMS further
#get-url = "http://127.0.0.1/sms-testing/index.php?phone=%p&text=%a"
#exec = <PathToScripts>/record_args.sh "%p" "%m" "%M" "%C" "%u" "%b"
get-url = "http://localhost/sms/index.php?t=%t&q=%q&a=%a"
# do not send anything back
#max-messages = 0
concatenation = true

# SMS SERVICE 'Default'
# there should be default always
group = sms-service
keyword = xxxxxxse
#catch-all = true
#exec = /usr/local/bin/kannel_incoming %t %q %a
#get-url = "http://localhost/sms/index1.php?t=%t&q=%q&a=%a"
text="Hello"
max-messages = 0
concatenation = true

# SMS sending
group = sendsms-user
username = sms
password = sms
user-allow-ip = "127.0.0.1"
default-smc = "ES75"
concatenation = true

# DLR with MySQL support configuration
#

```

```
# Example defining a MySQL database connection resource and
# the required table and field values.
#
group = mysql-connection
id = mydlr
host = localhost
username = root
password =
database = ncc_water
# max count of connections that will be opened for dbpool
# default is 1
max-connections = 1
```

```
group = dlr-db
id = mydlr
table = delivery_reports
field-smsc = smsc
field-timestamp = ts
field-destination = destination
field-source = source
field-service = service
field-url = url
field-mask = mask
field-status = status
field-boxc-id = boxc
```

sqlbox1.conf configuration file for sqlbox service

```
group = sqlbox
id = sqlbox-db
smsbox-id = smsbox
bearerbox-host = localhost
bearerbox-port = 13001
smsbox-port = 13003
smsbox-port-ssl = false
sql-log-table = sent_sms
sql-insert-table = send_sms
log-file = "/var/log/kannel/kannel-sqlbox.log"
log-level = 0
```

```
group = mysql-connection
id = sqlbox-db
host = localhost
username = root
password =
database = ncc_water
max-connections = 10
```

APPENDIX B: KANNEL INSTALLATION

Downloading and Compiling

You need to download and compile kannel. You visit [the Kannel.org website](http://www.kannel.org) and download the latest and greatest *gateway-1.X.Y.tar.gz* file.

From there:

```
# mkdir src
# cd src
# tar xzf ../downloads/gateway-1.4.1.tar.gz
# cd gateway-1.4.1
# configure --prefix=/usr/local/kannel
```

Compile and install.

```
# make
# sudo make install
password: *****
```

the sqlbox is different and should be downloaded separately and installed as above

Running the Server

After developing the hardest part of all configuration files run the kannel using the following commands

```
# cd /usr/local/kannel
# cp ~/src/gateway-1.4.1/smskannel.conf .
# cp ~/src/gateway-1.4.1/gw/modems.conf .
# sbin/bearerbox -v 0 smskannel.conf &
# sbin/wapbox -v 0 wap.conf &
# sbin/sqlbox -v 0 sqlbox.conf &
# sbin/smsbox -v 0 smskannel.conf &
```

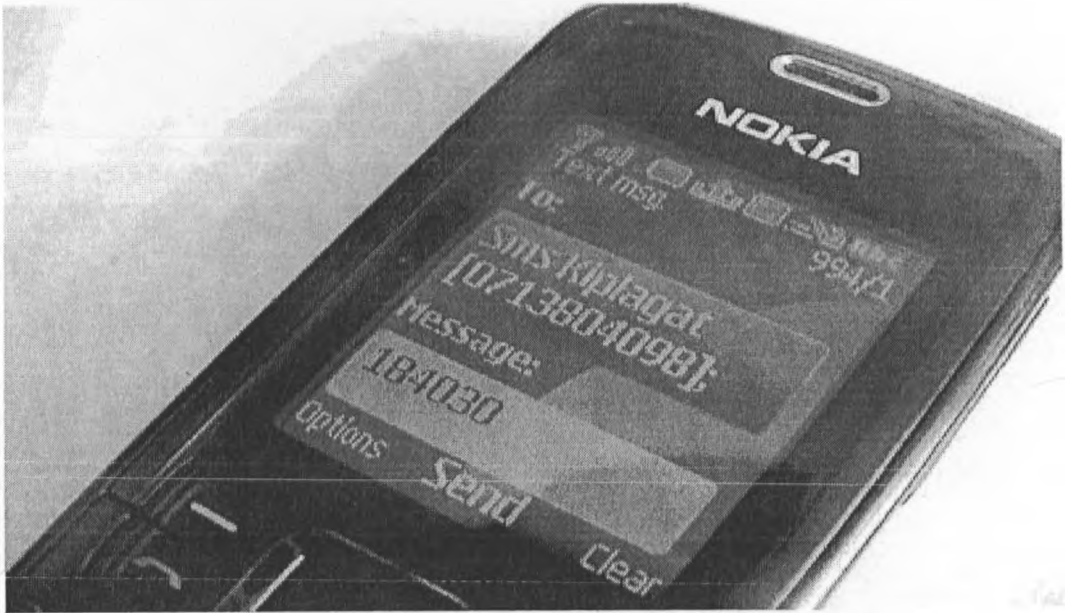
I tend to run the last two commands in two separate shell windows when developing/debugging so that I can see the output from the two programs clearly and use the information to help me figure out what's going on (level 0 really tells you a lot).

APPENDIX C: PROTOTYPE USER MANUAL

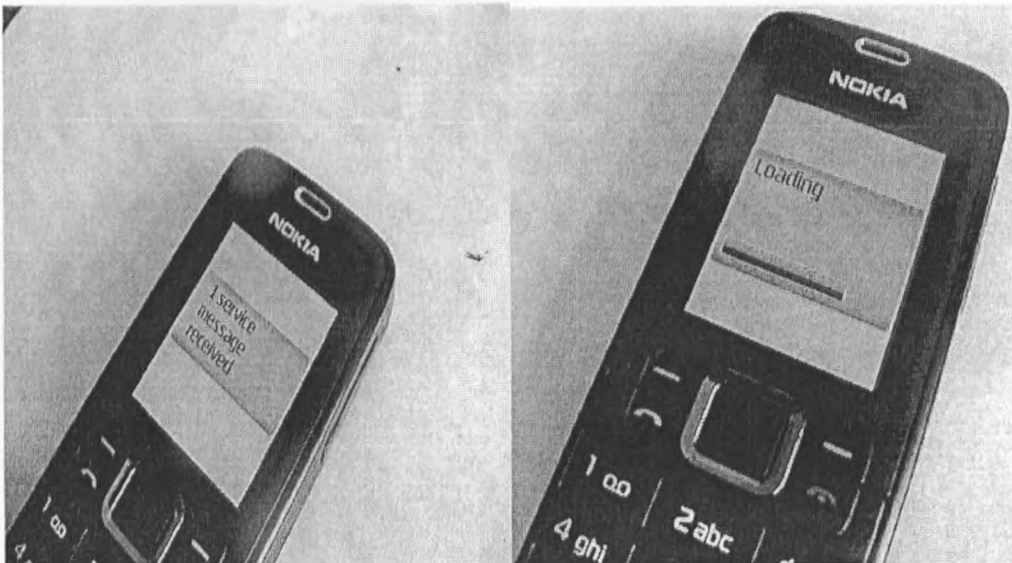
Using the mobile data collection system

Two way channel authentication

- a) Send a message to **0713-804-098** containing the payroll number supplied in table 1.4 to establish session ID, for 2 way channel of authentication mechanism and receive the system access address.

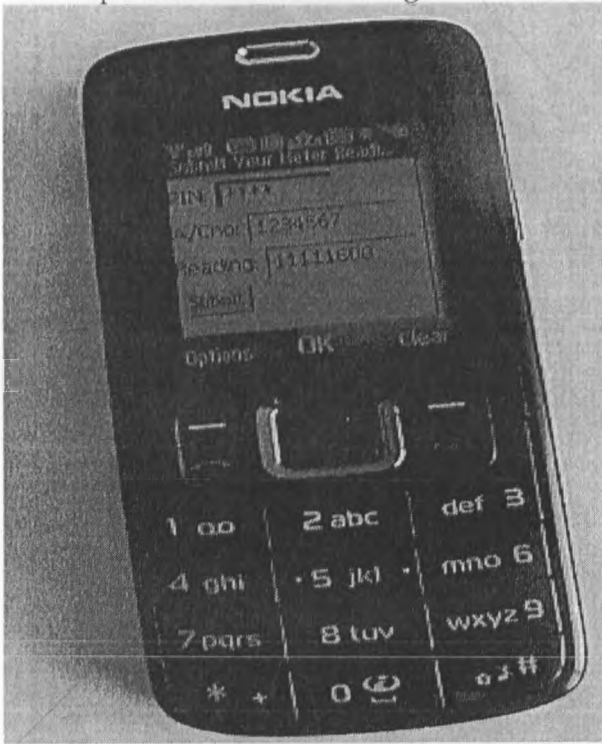


- b) A Service Message will send to your registered mobile phone. Click on it to access the meter reading system. Note that the session is currently set for a maximum of 10 minutes.



Mobile Meter Reading

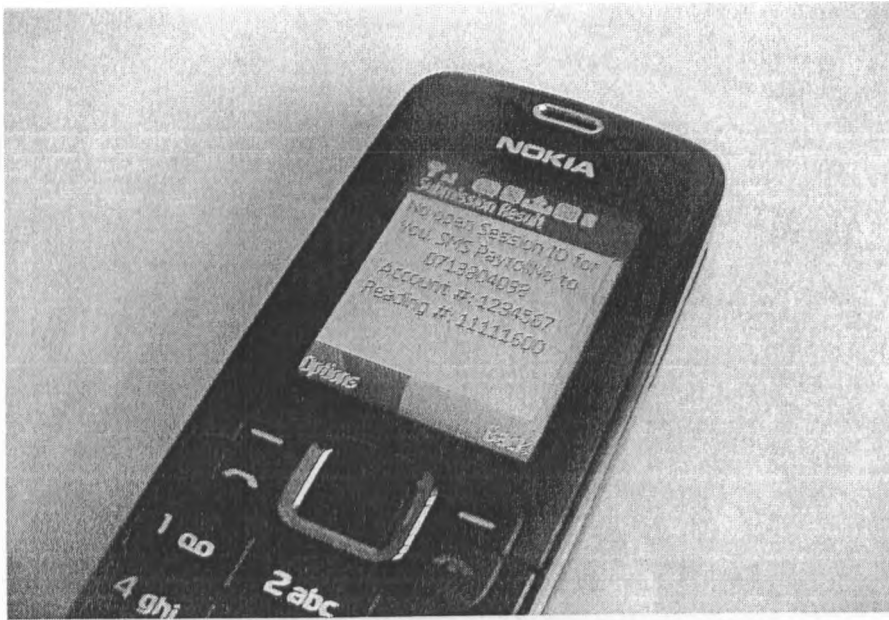
- c) A form will be displayed. Fill your PIN, Customer A/C number and Meter reading based on sample data in table 1.4 for each user as per the number of times the test is being done. I.e. if you are testing for the fifth time, enter the meter reading shown on the fifth test. And click on submit button to post the meter reading



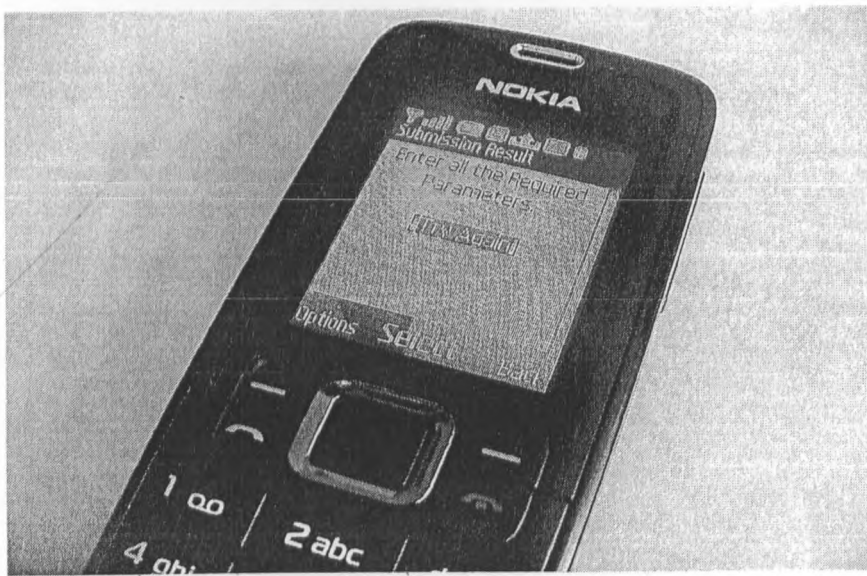
If successful a dialogue below will be displayed



If session is not open a dialogue below will be displayed with a link to go back



if invalid entries a dialogue below will be displayed



Customer Information Service

- d) On receiving confirmation dialogue check the email of the customer supplied to confirm that he has received the bill as per the message received.

Confirmation SMS Message to customer while meter reader still at the customer premise.



Customer Monthly Bill statement download from his/her Email account

NAIROBI WATER COMPANY
SERVING THE PEOPLE OF NAIROBI

MONTHLY STATEMENT FOR THE MONTH OF JULY 2008 (Closed) 22-Jul-2008 12:07 pm

Account Number: 1234567 Name: PAUL KARIUKI

Trans Date	Description	DEBIT	CREDIT
2008-07-09 12:33:08	WATER BILL PAYMENT(KSHS)		1,000.00
2008-07-09 17:28:09	WATER BILL INVOICE(KSHS)	449.00	
2008-07-09 17:34:02	WATER BILL INVOICE(KSHS)	113.00	
2008-07-09 17:43:45	WATER BILL INVOICE(KSHS)	288.00	
2008-07-09 17:49:46	WATER BILL INVOICE(KSHS)	113.00	
2008-07-09 18:01:34	WATER BILL INVOICE(KSHS)	978.00	
2008-07-09 20:12:33	WATER BILL INVOICE(KSHS)	230.00	
2008-07-10 06:09:39	WATER BILL INVOICE(KSHS)	2,300.00	
2008-07-10 13:32:51	WATER BILL INVOICE(KSHS)	-1,130.00	
2008-07-10 15:31:37	WATER BILL INVOICE(KSHS)	-4,600.00	
2008-07-22 11:47:24	WATER BILL INVOICE(KSHS)	-2,300.00	
Tue-Jul-2008	Total	5,625.00	5,000.00
	Balance	625.00	

Sent By : nairobi@nwc.co.ke

Approved By : NAIROBI WATER COMPANY
NCC ACCOUNT

Errors and Omissions Expected. All Queries Email the Undersigned.

System Administration module

To aid in the system administration, we developed a web interface for the administrator to be able to add users manage meter readers mobile phones, customers and employees.

Login to administrative module

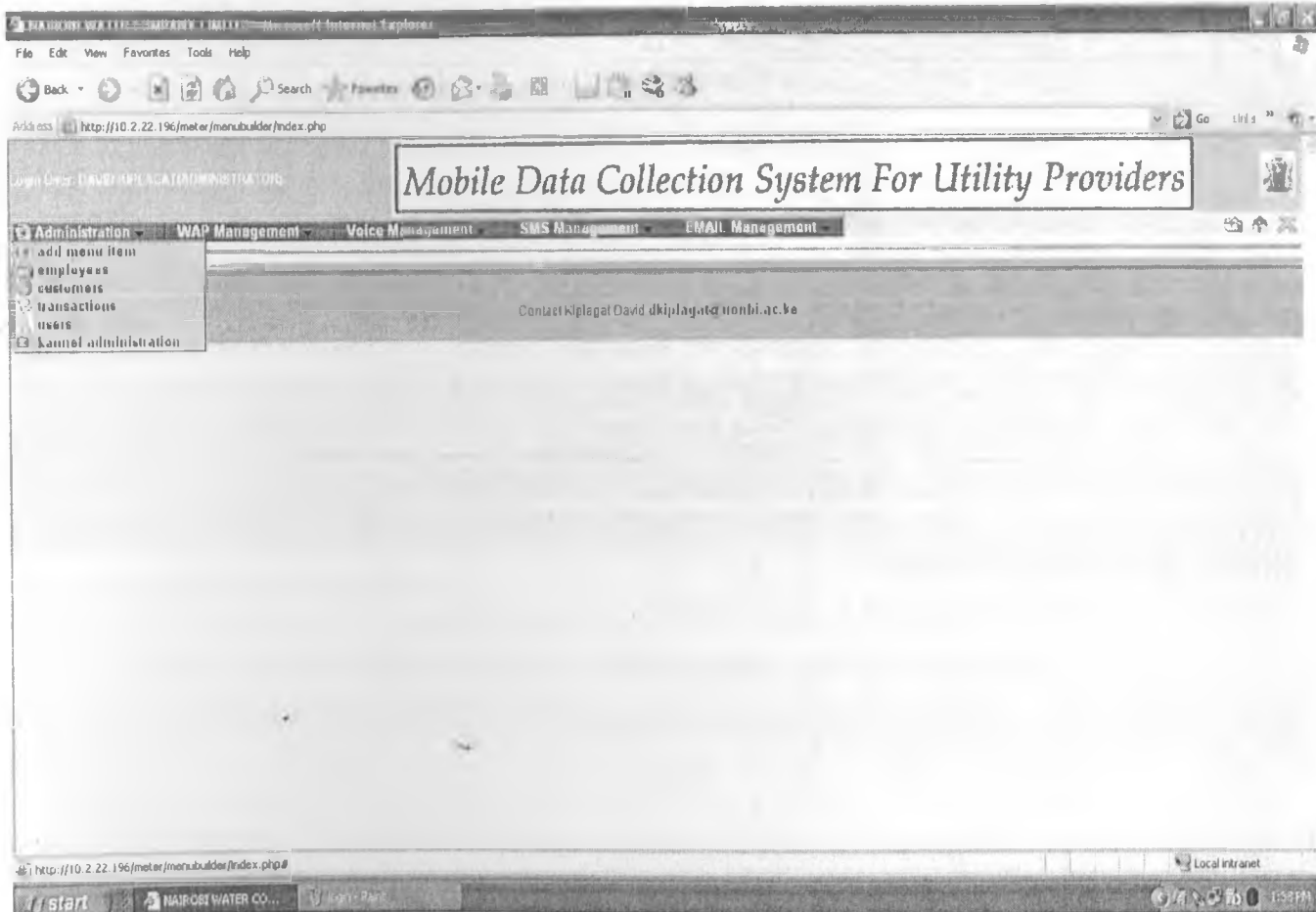
MOBILE DATA COLLECTION SYSTEM MGMT

Username

Password

MSC. COMP SCIENCE

On login the main web page containing the menu to various functions as shown below;



Adding Records

A custom for was prepared using Ajax forms to add users, customers and administrators to the system the form is shown below.

Add record	
ID	
Name	
PayrollNo	
Status	Active
MobileNo	
Email	
Save Cancel	

Editing Records

A custom for was prepared using Ajax forms to update users, customers and administrators to the system the form is shown below.

Edit record	
ID	1
Name	PAUL KARIUKI
Accountno	1234567
Status	Active
MobileNo	254720788012
Email	dkiplagat@uonbi.ac.ke
Save Cancel	

Checking established sessions

To view the users who are currently have connected to the system you click on the menu the sessions. You will be able to view the status of all the sessions established and there status as show below

http://10.7.22.196/micr/menubuilder/datagrid/sessions.php - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Search Favorites

http://10.7.22.196/micr/menubuilder/datagrid/sessions.php

Mobile Data Collection System For Utility Providers

ID	Name	sessionDate	PayrollNo	Status	MobileNo	Security_code
5	DAVID KIPLAGAT	2008-07-09 17:49:46	184030	Closed	+254720788012	253614bbac999b38b5b60cae531c4969
8	DAVID KIPLAGAT	2008-07-10 08:09:39	184030	Closed	+254720788012	253614bbac999b38b5b60cae531c4969
11	DAVID KIPLAGAT	2008-07-10 15:51:57	184030	Closed	+254720788012	253614bbac999b38b5b60cae531c4969
14	DAVID KIPLAGAT	2008-07-22 15:36:34	184030	Closed	+254720788012	253614bbac999b38b5b60cae531c4969
3	DAVID KIPLAGAT	2008-07-09 17:34:02	184030	Closed	+254720788012	253614bbac999b38b5b60cae531c4969
17	DAVID KIPLAGAT	2008-07-24 16:54:15	184030	Open	+254720788012	253614bbac999b38b5b60cae531c4969
6	DAVID KIPLAGAT	2008-07-09 18:01:34	184030	Closed	+254720788012	253614bbac999b38b5b60cae531c4969
9	DAVID KIPLAGAT	2008-07-10 08:09:39	184030	Closed	+254720788012	253614bbac999b38b5b60cae531c4969
12	DAVID KIPLAGAT	2008-07-22 11:47:24	184030	Closed	+254720788012	253614bbac999b38b5b60cae531c4969
1	DAVID KIPLAGAT	2008-07-09 17:21:41	184030	Closed	+254720788012	253614bbac999b38b5b60cae531c4969
15	DAVID KIPLAGAT	2008-07-22 15:36:42	184030	Closed	+254720788012	253614bbac999b38b5b60cae531c4969
4	DAVID KIPLAGAT	2008-07-09 17:45:43	184030	Closed	+254720788012	253614bbac999b38b5b60cae531c4969
7	DAVID KIPLAGAT	2008-07-09 20:12:33	184030	Closed	+254720788012	253614bbac999b38b5b60cae531c4969
10	DAVID KIPLAGAT	2008-07-10	184030	Closed	+254720788012	253614bbac999b38b5b60cae531c4969

Done Local intranet

start

There are quite a number of other administrative functions that can be viewed which are self explanatory from the main menu.

APPENDIX D: CODE SAMPLES

Refer to the attached CD-ROM for complete Code for mobile data collection system.

APPENDIX E: USABILITY ANALYSIS EXPERIMENT AND QUESTIONNAIRE

Approval letter of authority to conduct research



NAIROBI CITY WATER & SEWERAGE COMPANY LTD.

KAMPALA RD P. O. Box 30656 GPO 00100, Nairobi
TEL: 557131/2/3/552150/553737
FAX: 552126 / 552133
EMAIL: info@nairobiwater.co.ke
WEBSITE: www.nairobiwater.co.ke

NCWSC/HR/TRG.13/Vol.1/13/PMK

19th August, 2008

David Kiplagat
University of Nairobi
P.O Box 30197 - 00100
Nairobi

Dear Sir,

RE: RESEARCH PROJECT "USABILITY TEST FOR MOBILE METER READING SYSTEM"

Reference is made to your letter dated 14th August, 2008 on the above subject.

We write to confirm that Nairobi City Water & Sewerage Co. Ltd has granted you authority to carry out the above mentioned research in our **Commercial Directorate**.

You are kindly requested to forward a copy of the research upon completion of the exercise to the HR Manager. Please report to the **Billing Manager – Kampala Rd**

By a copy this letter the above manager will assist you with the relevant information.

Yours faithfully,


Grace W Ndungu (Ms)
Human Resource Manager

*Am (Central)
Kindly assist the
Bureau. He does good
ideas that can work
for
01/09/2008*

Usability analysis experiment and questionnaire

This questionnaire and usability experiment is prepared and sent to you to enable me gather information from the intended users on the usability of the mobile data collection system for utility providers. The objective of the study and experiment is to conduct usability analysis of the system to enable come up with recommendation that will assist the industry in further enhancing this research project for the benefit of the intended organization. I would be very grateful if you would take a while and respond to the questionnaire after conducting the experiment. I wish to assure you that the information gathered will be considered strictly confidential and will therefore not be used for any other purpose other than seeking to fulfill academic requirements for award of a degree.

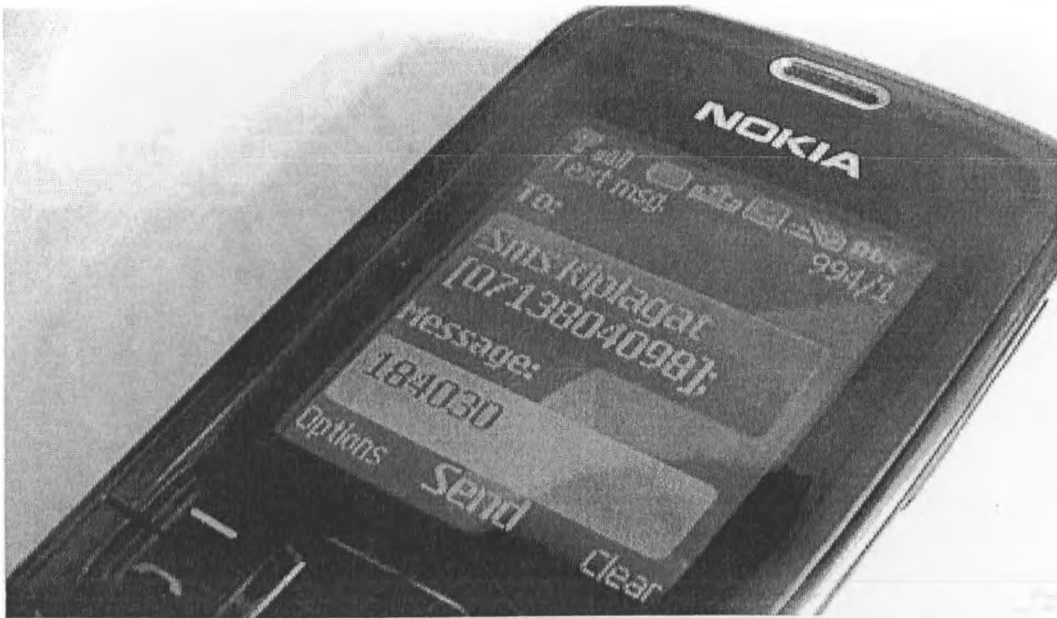
Please feel free to contact me on my mail address: dkiplagat@uonbi.ac.ke or cell phone 0720788012 or 020-3505889 or visit our web portal for this research at http://41.204.186.73/usability_test.php should any of the questions or experimental procedure not clear.

USERBILITY TESTING EXPERIMENT

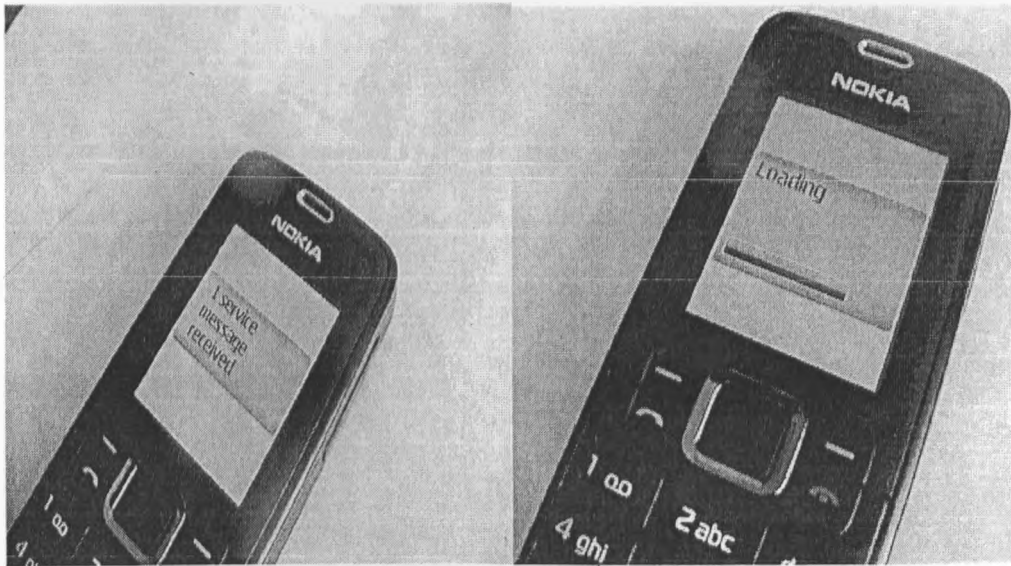
Using you WAP enabled phone, you are supposed to repeat the task/operation below 5 times using test data given in table 1.4 below or the companies test sample data which the customer account details have to be registered in the test system. Please perform these at a pace that feels natural to you. As you do so, note on the supplied piece of paper any errors and difficulty noted, the feeling of what you think could have been done better and any general recommendation and comments. This should be done after completing the task. The airtime used will be reimbursed where SMS cost Ksh 3.50 or GRPS message Ksh 1.0 and WAP system access is a total of 3KB = Ksh 0.03 as per the Safaricom charges. Also note that all mobile to be used have to be registered to be able to access the system.

Task Procedure

- e) Send a message to **0713-804-098** containing the payroll number supplied in table 1.4 to establish session ID, for 2 way channel of authentication mechanism and receive the system access address.



- f) A Service Message will send to your registered mobile phone. Click on it to access the meter reading system. Note that the session is currently set for a maximum of 10 minutes.



- g) A form will be displayed. Fill your PIN, Customer A/C number and Meter reading based on sample data in table 1.4 for each user as per the number of times the test is being done. I.e. if you are testing for the fifth time, enter the meter reading shown on the fifth test. And click on submit button to post the meter reading



h) On receiving confirmation dialogue check the email of the customer supplied to confirm that he has received the bill as per the message received.

Confirmation SMS Message to customer while meter reader still at the customer premise.



Customer Monthly Bill statement download from his/her Email account

**NAIROBI WATER COMPANY
SERVING THE PEOPLE OF NAIROBI**

MONTHLY STATEMENT FOR THE MONTH OF JULY 2008 Printed: 22-Jul-2008 13:07 pm

Account Number: 1234567 Name: PAUL KARIUKI

Trans Date	Description	DEBIT	CREDIT
2008-07-09 12:52:08	WATER BILL PAYMENT(KSHS)		5,000.00
2008-07-09 17:38:09	WATER BILL INVOICE(KSHS)	449.00	
2008-07-09 17:34:03	WATER BILL INVOICE(KSHS)	115.00	
2008-07-09 17:43:48	WATER BILL INVOICE(KSHS)	288.00	
2008-07-09 17:49:46	WATER BILL INVOICE(KSHS)	115.00	
2008-07-09 18:01:34	WATER BILL INVOICE(KSHS)	978.00	
2008-07-09 20:12:33	WATER BILL INVOICE(KSHS)	230.00	
2008-07-10 08:09:39	WATER BILL INVOICE(KSHS)	2,300.00	
2008-07-10 13:12:31	WATER BILL INVOICE(KSHS)	-1,150.00	
2008-07-10 15:31:37	WATER BILL INVOICE(KSHS)	4,600.00	
2008-07-22 11:47:24	WATER BILL INVOICE(KSHS)	-2,300.00	
Tue-Jul-2008	Total	5,625.00	5,000.00
	Balance	625.00	

Sent By: customer@nwc.ac.ke

Approved By: NAIROBI WATER COMPANY
NWC ACCOUNT

Errors and Omissions Expected. All Queries Email the Underigned

USERBILITY TEST DATA

**Table 1.4: Usability Test Run Data
Userbility Experiment**

Customer Test Email: customer_nwc@uonbi.ac.ke

Customer Test Mobile No: 0720788012

Payroll No	PIN	Mobile Model	Test Mobile No.	Customer A/C	Customer Meter Reading					Remarks
					Test1	Test2	Test3	Test4	test5	
184030	2012	N3110c	0720788012	1234567	11112000	11112050	11112100	11112150	11112200	
184031	2013			1234568	11113000	11113050	11113100	11113150	11113200	
184032	2014			1234569	11114000	11114050	11114100	11114150	11114200	
184033	2015			1234570	11115000	11115050	11115100	11115150	11115200	
184034	2016			1234571	11116000	11116050	11116100	11116150	11116200	
184035	2017			1234572	11117000	11117050	11117100	11117150	11117200	
184036	2018			1234573	11118000	11118050	11118100	11118150	11118200	
184037	2019			1234574	11119000	11119050	11119100	11119150	11119200	
184038	2020			1234575	11120000	11120050	11120100	11120150	11120200	
184039	2021			1234576	11121000	11121050	11121100	11121150	11121200	
184040	2022			1234577	11122000	11122050	11122100	11122150	11122200	
184041	2023			1234578	11123000	11123050	11123100	11123150	11123200	
184042	2024			1234579	11124000	11124050	11124100	11124150	11124200	
184043	2025			1234580	11125000	11125050	11125100	11125150	11125200	
184044	2026			1234581	11126000	11126050	11126100	11126150	11126200	
184045	2027			1234582	11127000	11127050	11127100	11127150	11127200	
184046	2028			1234583	11128000	11128050	11128100	11128150	11128200	
184047	2029			1234584	11129000	11129050	11129100	11129150	11129200	
184048	2030			1234585	11130000	11130050	11130100	11130150	11130200	
184049	2031			1234586	11131000	11131050	11131100	11131150	11131200	
184050	2032			1234587	11132000	11132050	11132100	11132150	11132200	
184051	2033			1234588	11133000	11133050	11133100	11133150	11133200	

184052	2034			1234589	11134000	11134050	11134100	11134150	11134200	
184053	2035			1234590	11135000	11135050	11135100	11135150	11135200	
184054	2036			1234591	11136000	11136050	11136100	11136150	11136200	
184055	2037			1234592	11137000	11137050	11137100	11137150	11137200	
184056	2038			1234593	11138000	11138050	11138100	11138150	11138200	
184057	2039			1234594	11139000	11139050	11139100	11139150	11139200	
184058	2040			1234595	11140000	11140050	11140100	11140150	11140200	
184059	2041			1234596	11141000	11141050	11141100	11141150	11141200	
184060	2042			1234597	11142000	11142050	11142100	11142150	11142200	
184061	2043			1234598	11143000	11143050	11143100	11143150	11143200	
184062	2044			1234599	11144000	11144050	11144100	11144150	11144200	
184063	2045			1234600	11145000	11145050	11145100	11145150	11145200	

QUESTIONNAIRE

A. Demography

Participant No.: _____

1. Gender: Female Male
2. Have you ever used a phone? no yes If yes: Model:_____ How long: _____
3. Age: Below 20 21-30 31-40 41-50 Above 50
4. Education Level: 'O' level 'A' level Bachelor degree/ Diploma Master degree and above

B. Survey Questions on the Usability of Mobile Data Collection System

Use a 5-point Likert scale where. 1=strongly disagree, 2=Disagree, 3=neither agree nor disagree, 4=Agree, 5=strongly agree. Indicate on the corresponding grid supplied using a tick (√)

#	Survey Questions	[1]	[2]	[3]	[4]	[5]
1	The visual size of the application is suitable					
2	The form design is clear and simple					
3	The speed of the system is fast enough					
4	It is easy to get the menu for task execution					
5	Its is easy to carry out task					
6	It is easy to get out on error					
7	it is easy to enter data easily and quickly					
8	It is convenient to fill out the meter reading form					

9	It is fast to get a response on submitting the meter reading					
10	It is easy to rectify the errors committed					
11	It provides flexible user guidance					
12	It is easy to know what to do next with this application					
13	It is easy to recall how to do things within this application					
14	It is easy to move from one part of a task to another					
15	It is easy to see at a glance what the options are at each stage					
16	Audio feedback is required					
17	It is comfortable to use the application					
18	The ordering of menu options is logical					
19	The application very attractive presentation					
20	I am happy with the application service					
21	I will often prefer the mobile data collection system					
22	It is a convenient and efficient way of mobile data collection for utility companies					
	Total					

General Comments

Transaction Logs

Transaction Logs						
#	User	Start Date	End Date	Reading	Security code	Time(sec)
1	184030	9/1/2008 16:45:41	9/1/2008 16:47:42	11112000	253614bbac999b38b5b60cae531c4969	121
1	184030	9/1/2008 16:40:12	9/1/2008 16:42:13	11112000	253614bbac999b38b5b60cae531c4969	121
1	184030	9/1/2008 16:35:46	9/1/2008 16:37:47	11112000	253614bbac999b38b5b60cae531c4969	121
1	184030	9/1/2008 16:12:07	9/1/2008 16:14:08	11112000	253614bbac999b38b5b60cae531c4969	121
1	184030	9/1/2008 16:45:41	9/1/2008 16:48:58	11112050	253614bbac999b38b5b60cae531c4969	197
1	184030	9/1/2008 16:40:12	9/1/2008 16:43:29	11112050	253614bbac999b38b5b60cae531c4969	197

1	184030	9/1/2008 16:35:46	9/1/2008 16:39:03	11112050	253614bbac999b38b5b60cae531c4969	197
1	184030	9/1/2008 16:12:07	9/1/2008 16:15:24	11112050	253614bbac999b38b5b60cae531c4969	197
2	184031	9/17/2008 21:32:07	9/17/2008 21:33:15	11113050	8038da89e49ac5eabb489cfc6cea9fc1	68
2	184031	9/17/2008 21:32:01	9/17/2008 21:33:09	11113050	8038da89e49ac5eabb489cfc6cea9fc1	68
2	184031	9/17/2008 21:32:07	9/17/2008 21:35:52	11113200	8038da89e49ac5eabb489cfc6cea9fc1	225
2	184031	9/17/2008 21:32:01	9/17/2008 21:35:46	11113200	8038da89e49ac5eabb489cfc6cea9fc1	225
2	184031	9/17/2008 21:32:07	9/17/2008 21:35:10	11113000	8038da89e49ac5eabb489cfc6cea9fc1	183
2	184031	9/17/2008 21:32:01	9/17/2008 21:35:04	11113000	8038da89e49ac5eabb489cfc6cea9fc1	183
2	184031	9/17/2008 21:32:07	9/17/2008 21:34:55	11113050	8038da89e49ac5eabb489cfc6cea9fc1	168
2	184031	9/17/2008 21:32:01	9/17/2008 21:34:49	11113050	8038da89e49ac5eabb489cfc6cea9fc1	168
2	184031	9/17/2008 21:32:07	9/17/2008 21:33:40	11113100	8038da89e49ac5eabb489cfc6cea9fc1	93
2	184031	9/17/2008 21:32:01	9/17/2008 21:33:34	11113100	8038da89e49ac5eabb489cfc6cea9fc1	93
2	184031	9/17/2008 21:32:07	9/17/2008 21:34:41	11113100	8038da89e49ac5eabb489cfc6cea9fc1	154
2	184031	9/17/2008 21:32:01	9/17/2008 21:34:35	11113100	8038da89e49ac5eabb489cfc6cea9fc1	154
2	184031	9/17/2008 21:32:07	9/17/2008 21:35:58	11113200	8038da89e49ac5eabb489cfc6cea9fc1	231
2	184031	9/17/2008 21:32:01	9/17/2008 21:35:52	11113200	8038da89e49ac5eabb489cfc6cea9fc1	231
3	184032	9/16/2008 18:03:23	9/16/2008 18:04:39	11114000	cee8d6b7ce52554fd70354e37bbf44a2	76
3	184032	9/16/2008 18:03:23	9/16/2008 18:05:32	11114050	cee8d6b7ce52554fd70354e37bbf44a2	129
3	184032	9/16/2008 18:03:23	9/16/2008 18:07:16	11114100	cee8d6b7ce52554fd70354e37bbf44a2	233
3	184032	9/16/2008 18:03:23	9/16/2008 18:07:03	11114150	cee8d6b7ce52554fd70354e37bbf44a2	220
4	184033	9/16/2008 22:59:28	9/16/2008 23:01:05	11115000	65d2ea03425887a717c435081cfc5dbb	97
4	184033	9/16/2008 22:59:28	9/16/2008 23:01:32	11115050	65d2ea03425887a717c435081cfc5dbb	124
4	184033	9/16/2008 22:59:28	9/16/2008 23:03:13	11115100	65d2ea03425887a717c435081cfc5dbb	225
4	184033	9/16/2008 22:59:28	9/16/2008 23:02:16	11115150	65d2ea03425887a717c435081cfc5dbb	168
4	184033	9/16/2008 22:59:28	9/16/2008 23:01:38	11115200	65d2ea03425887a717c435081cfc5dbb	130
4	184033	9/16/2008 22:59:28	9/16/2008 23:01:24	11115250	65d2ea03425887a717c435081cfc5dbb	116
5	184034	9/16/2008 23:15:51	9/16/2008 23:19:14	11116000	95192c98732387165bf8e396c0f2dad2	203
5	184034	9/16/2008 23:15:51	9/16/2008 23:19:23	11116050	95192c98732387165bf8e396c0f2dad2	212
5	184034	9/16/2008 23:15:51	9/16/2008 23:18:40	11116100	95192c98732387165bf8e396c0f2dad2	169
5	184034	9/16/2008 23:15:51	9/16/2008 23:18:59	11116150	95192c98732387165bf8e396c0f2dad2	188
5	184034	9/16/2008 23:15:51	9/16/2008 23:18:34	11116200	95192c98732387165bf8e396c0f2dad2	163
6	184035	9/17/2008 5:55:55	9/17/2008 5:57:02	11117000	8d8818c8e140c64c743113f563cf750f	67
6	184035	9/17/2008 5:55:55	9/17/2008 5:58:34	11117000	8d8818c8e140c64c743113f563cf750f	159
6	184035	9/17/2008 5:55:55	9/17/2008 5:57:57	11117050	8d8818c8e140c64c743113f563cf750f	122
6	184035	9/17/2008 5:55:55	9/17/2008 5:59:50	11117100	8d8818c8e140c64c743113f563cf750f	235
6	184035	9/17/2008 5:55:55	9/17/2008 5:58:25	11117150	8d8818c8e140c64c743113f563cf750f	150
6	184035	9/17/2008 5:55:55	9/17/2008 5:58:20	11117200	8d8818c8e140c64c743113f563cf750f	145
7	184036	9/17/2008 7:25:06	9/17/2008 7:28:57	11118000	84ddf34126fc3a48ee38d7044e87276	231
7	184036	9/17/2008 7:25:06	9/17/2008 7:27:23	11118050	84ddf34126fc3a48ee38d7044e87276	137
8	184037	9/17/2008 10:10:11	9/17/2008 10:13:00	11119000	ea6b2efbdd4255a9f1b3bbc6399b58f4	169
8	184037	9/17/2008 10:10:11	9/17/2008 10:11:18	11119050	ea6b2efbdd4255a9f1b3bbc6399b58f4	67
9	184038	9/17/2008 10:44:34	9/17/2008 10:45:47	11120000	7b7a53e239400a13bd6be6c91c4f6c4e	73
9	184038	9/17/2008 10:44:34	9/17/2008 10:47:08	11120050	7b7a53e239400a13bd6be6c91c4f6c4e	154
10	184039	9/17/2008 11:11:41	9/17/2008 11:14:38	11121000	05a5cf06982ba7892ed2a6d38fe832d6	177
10	184039	9/17/2008 11:11:41	9/17/2008 11:15:37	11121050	05a5cf06982ba7892ed2a6d38fe832d6	236
11	184040	9/17/2008 11:43:00	9/17/2008 11:46:14	11122000	3a824154b16ed7dab899bf000b80e0000	194
11	184040	9/17/2008 11:43:00	9/17/2008 11:45:30	11122050	3a824154b16ed7dab899bf000b80e0000	150
12	184041	9/17/2008 13:00:07	9/17/2008 13:01:18	11123000	5531a583481622280f20d1ef9e95f69	71

12	184041	9/17/2008 13:00:07	9/17/2008 13:02:14	11123050	5531a5834816222280f20d1ef9e95f69	127
13	184042	9/17/2008 13:03:10	9/17/2008 13:04:22	11124000	07811dc6c422334ce36a09ff5cd6fe71	72
13	184042	9/17/2008 13:03:10	9/17/2008 13:05:13	11124050	07811dc6c422334ce36a09ff5cd6fe71	123
14	184043	9/17/2008 13:06:04	9/17/2008 13:07:08	11125000	312351bf07989769097660a56395065	64
14	184043	9/17/2008 13:06:04	9/17/2008 13:08:09	11125050	312351bf07989769097660a56395065	125
15	184044	9/18/2008 8:04:02	9/18/2008 8:05:05	11126000	c92a10324374fac681719d63979d00fe	63
15	184044	9/18/2008 8:04:02	9/18/2008 8:05:57	11126050	c92a10324374fac681719d63979d00fe	115
16	184045	9/18/2008 8:06:47	9/18/2008 8:07:59	11127000	9f62b8625f914a002496335037e9ad97	72
16	184045	9/18/2008 8:06:47	9/18/2008 8:08:52	11127050	9f62b8625f914a002496335037e9ad97	125
17	184046	9/18/2008 8:09:35	9/18/2008 8:10:34	11128000	d860edd1dd83b36f02ce52bde626c653	59
17	184046	9/18/2008 8:09:35	9/18/2008 8:12:07	11128050	d860edd1dd83b36f02ce52bde626c653	152
17	184046	9/18/2008 8:09:35	9/18/2008 8:13:27	11128100	d860edd1dd83b36f02ce52bde626c653	232
18	184047	9/18/2008 8:14:32	9/18/2008 8:15:32	11129000	093b60fd0557804c8ba0cbf1453da22f	60
18	184047	9/18/2008 8:14:32	9/18/2008 8:17:32	11129050	093b60fd0557804c8ba0cbf1453da22f	180
18	184047	9/18/2008 8:14:32	9/18/2008 8:18:03	11129100	093b60fd0557804c8ba0cbf1453da22f	211
19	184048	9/18/2008 8:25:41	9/18/2008 8:27:27	11130000	2d579dc29360d8bbfb4aa541de5afa9	106
19	184048	9/18/2008 8:25:41	9/18/2008 8:28:33	11130050	2d579dc29360d8bbfb4aa541de5afa9	172
20	184049	9/18/2008 8:29:15	9/18/2008 8:31:22	11131000	88ef51f0bf911e452e8dbb1d807a81ab	127
20	184049	9/18/2008 8:29:15	9/18/2008 8:32:15	11131050	88ef51f0bf911e452e8dbb1d807a81ab	180
20	184049	9/18/2008 8:29:15	9/18/2008 8:32:56	11131100	88ef51f0bf911e452e8dbb1d807a81ab	221
21	184050	9/18/2008 8:33:44	9/18/2008 8:35:00	11132000	5352696a9ca3397beb79f116f3a33991	76
21	184050	9/18/2008 8:33:44	9/18/2008 8:39:20	11132050	5352696a9ca3397beb79f116f3a33991	336
22	184051	9/18/2008 8:44:28	9/18/2008 8:45:43	11133000	a5a61717dddc3501cfd7f4e22d7dbaa	75
22	184051	9/18/2008 8:44:28	9/18/2008 8:46:31	11133050	a5a61717dddc3501cfd7f4e22d7dbaa	123
23	184052	9/18/2008 8:47:36	9/18/2008 8:48:45	11134000	d198bd736a97e7cecfdf8f4f2027ef80	69
23	184052	9/18/2008 8:47:36	9/18/2008 8:49:52	11134050	d198bd736a97e7cecfdf8f4f2027ef80	136
24	184053	9/18/2008 8:50:36	9/18/2008 8:51:34	11135000	2b0f658cbffd284984fb11d90254081f	58
24	184053	9/18/2008 8:50:36	9/18/2008 8:52:23	11135050	2b0f658cbffd284984fb11d90254081f	107
25	184054	9/18/2008 9:11:17	9/18/2008 9:12:09	11136000	f48c04ffab49ff0e5d1176244dfb65c	52
25	184054	9/18/2008 9:11:17	9/18/2008 9:13:14	11136050	f48c04ffab49ff0e5d1176244dfb65c	117
26	184055	9/18/2008 9:15:03	9/18/2008 9:16:24	11137000	23d2e1578544b172cca332ff74bddf5f	201
26	184055	9/18/2008 9:15:03	9/18/2008 9:17:06	11137050	23d2e1578544b172cca332ff74bddf5f	123
26	184055	9/18/2008 9:15:03	9/18/2008 9:19:08	11137100	23d2e1578544b172cca332ff74bddf5f	245
26	184055	9/18/2008 9:15:03	9/18/2008 9:18:10	11137150	23d2e1578544b172cca332ff74bddf5f	187
26	184055	9/18/2008 9:15:03	9/18/2008 9:17:37	11137200	23d2e1578544b172cca332ff74bddf5f	154
26	184055	9/18/2008 9:15:03	9/18/2008 9:16:55	11137500	23d2e1578544b172cca332ff74bddf5f	112
26	184055	9/18/2008 9:15:03	9/18/2008 9:16:40	11137300	23d2e1578544b172cca332ff74bddf5f	97
26	184055	9/18/2008 9:15:03	9/18/2008 9:16:21	11137250	23d2e1578544b172cca332ff74bddf5f	78
28	184057	9/17/2008 12:38:09	9/17/2008 12:41:04	11139000	a48564053b3c7b54800246348c7fa4a0	175
28	184057	9/17/2008 12:38:09	9/17/2008 12:43:06	11139050	a48564053b3c7b54800246348c7fa4a0	297
28	184057	9/17/2008 12:38:09	9/17/2008 12:44:45	11139100	a48564053b3c7b54800246348c7fa4a0	396
28	184057	9/17/2008 12:38:09	9/17/2008 12:45:49	11139150	a48564053b3c7b54800246348c7fa4a0	460
28	184057	9/17/2008 12:38:09	9/17/2008 12:46:48	11139200	a48564053b3c7b54800246348c7fa4a0	519
30	184059	8/29/2008 15:35:32	8/29/2008 15:37:18	11141000	89885ff2c83a10305ee08bd507c1049c	106
30	184059	8/29/2008 15:31:12	8/29/2008 15:32:58	11141000	89885ff2c83a10305ee08bd507c1049c	106
30	184059	8/29/2008 15:35:32	8/29/2008 15:38:01	11141050	89885ff2c83a10305ee08bd507c1049c	149
30	184059	8/29/2008 15:31:12	8/29/2008 15:33:41	11141050	89885ff2c83a10305ee08bd507c1049c	149
31	184060	8/29/2008 12:00:36	8/29/2008 12:03:14	11142000	71e09b16e21f7b6919bbfc43f6a5b2f0	158

31	184060	8/29/2008 11:58:16	8/29/2008 12:00:54	11142000	71e09b16e21f7b6919bbfc43f6a5b2f0	158
31	184060	8/29/2008 11:55:27	8/29/2008 11:58:05	11142000	71e09b16e21f7b6919bbfc43f6a5b2f0	158
31	184060	8/29/2008 11:52:45	8/29/2008 11:55:23	11142000	71e09b16e21f7b6919bbfc43f6a5b2f0	158
31	184060	8/29/2008 11:46:06	8/29/2008 11:48:44	11142000	71e09b16e21f7b6919bbfc43f6a5b2f0	158
31	184060	8/29/2008 12:00:36	8/29/2008 12:02:17	11142100	71e09b16e21f7b6919bbfc43f6a5b2f0	101
31	184060	8/29/2008 11:58:16	8/29/2008 11:59:57	11142100	71e09b16e21f7b6919bbfc43f6a5b2f0	101
31	184060	8/29/2008 11:55:27	8/29/2008 11:57:08	11142100	71e09b16e21f7b6919bbfc43f6a5b2f0	101
31	184060	8/29/2008 11:52:45	8/29/2008 11:54:26	11142100	71e09b16e21f7b6919bbfc43f6a5b2f0	101
31	184060	8/29/2008 11:46:06	8/29/2008 11:47:47	11142100	71e09b16e21f7b6919bbfc43f6a5b2f0	101
31	184060	8/29/2008 12:00:36	8/29/2008 12:02:09	11142150	71e09b16e21f7b6919bbfc43f6a5b2f0	93
31	184060	8/29/2008 11:58:16	8/29/2008 11:59:49	11142150	71e09b16e21f7b6919bbfc43f6a5b2f0	93
31	184060	8/29/2008 11:55:27	8/29/2008 11:57:00	11142150	71e09b16e21f7b6919bbfc43f6a5b2f0	93
31	184060	8/29/2008 11:52:45	8/29/2008 11:54:18	11142150	71e09b16e21f7b6919bbfc43f6a5b2f0	93
31	184060	8/29/2008 11:46:06	8/29/2008 11:47:39	11142150	71e09b16e21f7b6919bbfc43f6a5b2f0	93
31	184060	8/29/2008 12:00:36	8/29/2008 12:01:37	11142200	71e09b16e21f7b6919bbfc43f6a5b2f0	61
31	184060	8/29/2008 11:58:16	8/29/2008 11:59:17	11142200	71e09b16e21f7b6919bbfc43f6a5b2f0	61
31	184060	8/29/2008 11:55:27	8/29/2008 11:56:28	11142200	71e09b16e21f7b6919bbfc43f6a5b2f0	61
31	184060	8/29/2008 11:52:45	8/29/2008 11:53:46	11142200	71e09b16e21f7b6919bbfc43f6a5b2f0	61
31	184060	8/29/2008 11:46:06	8/29/2008 11:47:07	11142200	71e09b16e21f7b6919bbfc43f6a5b2f0	61
31	184060	8/29/2008 12:00:36	8/29/2008 12:02:13	11142050	71e09b16e21f7b6919bbfc43f6a5b2f0	97
31	184060	8/29/2008 11:58:16	8/29/2008 11:59:53	11142050	71e09b16e21f7b6919bbfc43f6a5b2f0	97
31	184060	8/29/2008 11:55:27	8/29/2008 11:57:04	11142050	71e09b16e21f7b6919bbfc43f6a5b2f0	97
31	184060	8/29/2008 11:52:45	8/29/2008 11:54:22	11142050	71e09b16e21f7b6919bbfc43f6a5b2f0	97
31	184060	8/29/2008 11:46:06	8/29/2008 11:47:43	11142050	71e09b16e21f7b6919bbfc43f6a5b2f0	97
33	184062	9/2/2008 6:50:10	9/2/2008 6:51:39	11144000	d8330f857a17c53d217014ee776bfd50	89
33	184062	9/2/2008 6:50:10	9/2/2008 6:51:28	11144050	d8330f857a17c53d217014ee776bfd50	78
33	184062	9/2/2008 6:50:10	9/2/2008 6:51:37	11144100	d8330f857a17c53d217014ee776bfd50	87
33	184062	9/2/2008 6:50:10	9/2/2008 6:52:02	11144150	d8330f857a17c53d217014ee776bfd50	112
33	184062	9/2/2008 6:50:10	9/2/2008 6:51:17	11144200	d8330f857a17c53d217014ee776bfd50	67
34	184063	9/17/2008 12:38:17	9/17/2008 12:42:17	11145000	0189caa552598b845b29b17a427692d1	240
34	184063	9/17/2008 12:38:17	9/17/2008 12:43:33	11145050	0189caa552598b845b29b17a427692d1	316
34	184063	9/17/2008 12:38:17	9/17/2008 12:44:19	11145100	0189caa552598b845b29b17a427692d1	362
34	184063	9/17/2008 12:38:17	9/17/2008 12:45:02	11145150	0189caa552598b845b29b17a427692d1	405
34	184063	9/17/2008 12:38:17	9/17/2008 12:45:30	11145200	0189caa552598b845b29b17a427692d1	433

Survey Questionnaire Raw Results

Question Description	Dimension	Usability_Attributes	PARTICIPANTS																																	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	
The visual size of the application is suitable	Perception	size	5	3	5	4	5	5	4	4	5	3	3	4	4	5	3	5	4	5	4	4	5	5	3	4	3	5	5	5	4	4	1	3	4	
The form design is clear and simple		visibility	5	3	5	4	5	4	4	4	5	3	4	5	5	5	4	5	4	5	4	4	4	4	5	4	4	4	4	5	5	4	4	1	5	4
The speed of the system is fast enough	Control/Action	Speed	5	5	5	4	5		5	4	5	3	4	5	5	5	5	4	4	4	4	4	5	5	4	5	5	4	5	4	5	5	4	2	5	4
It is easy to get the menu for task execution		Simplicity	5	5	5	5	5	3	4	5	5	3	4	5	5	4	4	4	4	5	5	4	3	5	5	5	4	3	5	5	4	4	3	3	4	
Its easy to carry out task		comprehensibility	4	5	5	4	5	3	5	4	4	4	4	4	5	5	4	4	5	5	5	5	4	4	4	5	4	5	5	4	3	3	2	3	5	
It is easy to get out on error		Reliability	4	3	4	5	5	3	5	3	5	4	4	4	3	5	5	4	4	5	4	4	5	5	5	5	5	5	3	3	3	3	2	3	3	
it is easy to enter data easily and quickly		data capture	3	2	4	3	5	4	4	3	4	4	3	5	5	5	4	5	5	5	4	3	5	5	4	4	3	5	5	5	4	3	3	4	5	
It is convenient to fill out the meter reading form		Efficiency	3	3	4	3	5	5	5	3	5	5	3	5	3	5	4	5	4	5	4	4	5	5	4	4	5	4	5	5	2	4	1	4	4	
It is fast to get a response on submitting the meter reading		Responsiveness	5	2	5	5	5	5	5	5	3	5	4	5	3	5	3	3	5	3	4	4	3	5	3	4	3	5	4	4	5	4	1	5	5	
It is easy to rectify the errors committed		Rectification	3	4	5	1	5	5	5	4	3	3	1	4	3	5	3	5	4	3	4	4	4	5	3	4	5	5	5	4	3	3	5	3	3	
It provides flexible user guidance		Guidance	3	4	5	3	5	4	4	4	4	3	1	4	4	5	4	5	4	5	4	5	4	5	4	4	5	5	5	5	4	3	4	2	4	3
It is easy to know what to do next with this application		Capability	3	4	4	3	5	4	4	4	5	3	1	3	3	4	4	5	4	3	4	5	4	4	4	4	5	4	5	5	5	4	2	3	2	4
It is easy to recall how to do things within this application	predictability	4	4	5	5	5	4	4	5	5	3	2	4	4	5	4	5	5	4	4	4	4	5	5	5	5	5	5	5	4	3	3	3	4	4	
It is easy to move from one part of a task to another	Memorability	2	5	4	3	5	4	5	4	5	3	3	5	4	5	3	5	4	4	4	5	4	5	4	5	5	3	5	4	3	4		3	3		
It is easy to see at a glance what the options are at each stage	consistency	5	4	4	4	5	5	5	5	5	3	4	4	5	4	3	5	4	4	4	4	4	4	4	4	4	5	4	5	2	4	3	1	4	3	3
Audio feedback is required	Informative	1	3	4	3	5	5	5	4	5	4	3	3	3	5	3	4	4	5	3	4	4	4	4	4	4	5	5	5	1	5	5	5	1	5	3
It is comfortable to use the application	Reponsive	3	5	5	5	5	4	4	4	4	3	3	4	4	4	4	5	5	5	4	5	4	4	4	4	5	5	3	5	4	4	4	4	2	4	3
The ordering of menu options is logical	Comfort	3	5	5	3	5	3	4	4	4	3	3	3	4	4	4	5	5	3	5	5	4	5	5	4	5	5	4	4	3	4	2	4	4		
The application very attractive presentation	Logic	3	3	3	4	5	4	5	5	4	4	4	4	5	5	4	4	4	5	5	5	5	4	5	4	3	3	4	4	4	3	1	4	3		
I am happy with the application service	Attractiveness	3	5	5	4	5	5	4	4	5	3	5	5	4	5	5	5	4	5	5	4	4	5	5	4	3	5	5	4	5	4	1	3	3		
I will often prefer the mobile data collection system	Satisfaction	5	3	4	4	5	5	3	4	5	3	4	5	4	5	5	5	4	4	5	5	4	4	4	4	4	2	5	4	4	4	1	5	4		
It is a convenient and efficient way of mobile data	Acceptance	5	4	5	5	5	5	5	3	4	4	5	5	4	5	5	5	4	4	5	5	4	4	4	4	5	4	5	4	5	5	1	5	4		
	Convenience	5	4	5	5	5	5	5	3	4	4	5	5	4	5	5	5	4	4	5	5	4	4	4	4	5	4	5	4	5	5	1	5	4		

Cronbach's Alpha Calculation

Introduction

Reliability analysis allows you to study the properties of measurement scales and the items that make them up. The Reliability Analysis procedure calculates a number of commonly used measures of scale reliability and also provides information about the relationships between individual items in the scale. Interclass correlation coefficients can be used to compute interrater reliability estimates.

Example: Does my questionnaire measure customer satisfaction in a useful way? Using reliability analysis, you can determine the extent to which the items in your questionnaire are related to each other, you can get an overall index of the repeatability or internal consistency of the scale as a whole, and you can identify problem items that should be excluded from the scale.

The internal reliability consistency value (Cronbach's Alpha) is given by

$$\alpha = \frac{N \cdot \bar{c}}{(\bar{v} + (N - 1) \cdot \bar{c})}$$

where N is the number of components (items or testlets), \bar{v} equals the average variance and \bar{c} is the average of all covariances between the components

Calculation of cronbach's Alpha value for the four dimensions

Perception Reliability Test

***** Method 1 (space saver) will be used for this analysis *****

R E L I A B I L I T Y A N A L Y S I S - S C A L E (A L P H A)

Reliability Coefficients

N of Cases = 34.0

N of Items = 2

Alpha = .8558

Control/Action Reliability Test

***** Method 1 (space saver) will be used for this analysis *****

RELIABILITY ANALYSIS - SCALE (ALPHA)

Reliability Coefficients

N of Cases = 33.0 N of Items = 8

Alpha = .7082

Learning/Memorization Reliability Test

***** Method 1 (space saver) will be used for this analysis *****

RELIABILITY ANALYSIS - SCALE (ALPHA)

Reliability Coefficients

N of Cases = 33.0 N of Items = 6

Alpha = .7684

Evaluative Feeling Reliability Test

***** Method 1 (space saver) will be used for this analysis *****

RELIABILITY ANALYSIS - SCALE (ALPHA)

Reliability Coefficients

N of Cases = 34.0 N of Items = 6

Alpha = .8290

Overall Reliability Test

***** Method 1 (space saver) will be used for this analysis *****

RELIABILITY ANALYSIS - SCALE (ALPHA)

Reliability Coefficients

N of Cases = 32.0

N of Items = 22

Alpha = .8434