UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

PROJECT REPORT

POLICE SECURITY ENHANCEMENT VIA THE USAGE OF AN SMS GATEWAY IN NAIROBI

BY

DUNCAN OWINO MWAMBA

P56/71138/2008

Submitted in partial fulfilment for the requirements of Master of Science in Information Systems

May 2014

DECLARATION

I declare that this research is my original work and has not been submitted to any University or any institution of higher education.

Signature_____   _____

Duncan Owino Mwamba   **Date**

P56/71138/2008

I confirm that the work reported in this project was carried out by the candidate under my supervision.

Signature_____   _____

Prof. William Okello-Odongo   **Date**

Project Supervisor

School of Computing and Informatics

University of Nairobi

DEDICATION

To my pretty wife Mrs. Catherine Owino, for her encouragement and understanding during the hours away while working on this study.

To my brothers Dennis Omondi and Joseph Okwedo for their constant encouragements.

ACKNOWLEDGEMENT

I would like to sincerely express my gratitude to my supervisor, Professor William Okello-Odongo for the time and intellectual guidance he offered me during the study. He was truly devoted and professional.

To all lecturers and students who facilitated my learning experience and for their time we spent together.

To all the police officers and members of the public who provided me with the required information.

To all members of my family, friends, workmates at Ericsson Kenya and relatives for the support and encouragement they offered me during the study.

ABSTRACT

An SMS gateway is a telecommunications network facility for sending or receiving Short Message Service (SMS) transmissions to or from a telecommunications network that supports SMS. The main purpose of this study was to get the perception of both the police officers and members of the public in Nairobi on SMS gateway usage for the purpose of enhancing security. The research involved developing and implementing a prototype which permitted SMS communication using mobile phones between the police officers and members of the public. A survey using questionnaire was conducted to access the perceived impacts on both groups' experiences while using the SMS gateway. The study established that most police officers and members of public owned mobile phones and had long experience on daily SMS usage. Despite this, both groups mostly used face to face communication which was slow, manual and inconvenient to information flow. The study also established that SMS communication between the members of the public and the police officers was very rare. The same case applied to the intra-police SMS communication. Via the developed prototype, members of the public managed to easily send SMS to police stations. The police officers also managed to easily communicate internally via the gateway as well as send SMS to the members of the public. In terms of ease, convenience, speed and user friendliness in the processes of communicating security alerts, the system received high ratings from both groups. Finally future research directions on SMS gateway adoption and usage were discussed.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1.0: INTRODUCTION

1.1 BACKGROUND

As described by Azizinezhad et al (2012), SMS is an acronym used in the world of communications technology. It stands for Short Messaging Service which is a protocol used in communications that gives way to the exchange of short text messages from one mobile telephone device to another. SMS or text messaging largely dominates today's means of communication since seventy-four percent of all cell phone users send and receive text messages nowadays. The technology behind SMS has paved the way for the rapid growth of improvement of text messaging that has now allowed users to broadcast SMS text messages not just from mobile phones but also from computers with the use of SMS software and through public SMS gateways. The link between text messaging to SMS technology now co notates the terminology of "SMS" as the act of texting or sending text messages even with the use of a different communications protocol.

The use of SMS as an effective means of personal communication has expanded the market of text messaging. Businesses, government offices, and even television shows now use this service since SMS is the quickest way to get a message through from one entity to another. SMS text messaging is the most widely used data application on the planet, with 2.4 billion active users, or 74% of all mobile phone subscribers sending and receiving text messages on their phones . The SMS technology has facilitated the development and growth of text messaging. SMS has unique advantages that other non-voice services do not have. It provides a very convenient method of exchanging small bits of information between mobile users. The reasons for the enormous popularity of SMS have been the fact that this mechanism of sending and receiving messages not only saves time but costs less as well. In many situations one is relatively much more comfortable sending a message via SMS than talking over phone. With new information services and unique value added services being used by the operators the popularity of SMS is increasing further. SMS is also uniquely positioned as a very attractive advertisement medium. SMS should no longer be treated as a value added service in mobile networks. SMS is not only providing a useful mechanism for a host of innovative services over mobile networks but it acting as a point of entry for new data services like WAP in mobile networks (Azizinezhad et al,2012).

Common applications of SMS are:

- Exchanging small personal messages since it is much cheaper than calling someone and giving the same message. Calling someone to give the same message would invariably take more time and hence more cost.

- Offering e-mail services over SMS. Every user is assigned an e-mail address at signup and any message delivered to that email is converted to short messages and delivered to the mobile.

- Sending e-mail messages from a mobile phone to any e-mail address.

- Information services like news, weather, entertainment and stock prices etc. can be availed.

- SMS can be used by the network operators to provide services like balance enquiry in case of prepaid cards using SMS.

- Mobile chatting is one favourite application of SMS.

- SMS can be used to notify users that they have received new voice-mail or fax messages.

- It provides an alternative to alphanumeric paging services.

- Using SIM-Toolkit, now a part of GSM specifications, SMS can be used to have on the air activation of features. By sending codes embedded in short messages from the server network operators can remotely provision the user's wireless terminal.

- Internet e-mail alerts.

- Downloading new ring tones.

SMS is the most popular data bearer / service within GSM with an average of one billion SMS messages (at the end of 2002) transacted everyday around the world, with a growth of an average half a billion every month. The SS7 signalling channels are always physical present but mostly unused, be it in during an active user connection or in the idle state. It is therefore, quite an attractive proposition to use these channels for transmission of user data. SMS uses the free capacity of the signalling channel. Each SMS message is made up of 160 characters in length when 7-bit English characters are used. It is 140 octets when 8-bit characetrs (some European alphabets) are used, and 70 characters in length when non Latin alphabets such as Arabic, Chinese or Hindi are used (70 characters of 16 bit Unicode).

To use SMS as a bearer for information exchange, the origin server or the enterprise server needs to be connected to the SMSC (SMS Center) through a short message entity (SME). The SME in this case works as an SMS gateway, which interacts to the SMSC in one side and the enterprise server on the other side.

The main objective of this study is to get the perception of both the police officers and members of the public on SMS gateway usage for the purpose of enhancing security. The research will be to develop and implement a prototype which will enable various SMS communication capabilities using mobile devices. This SMS gateway will be deployed using Kannel on Linux Fedora 20. A survey will be conducted to access the perceived impact on both the police officers and members of the public and if this can increase the response and quality of communication within and outside the police stations. The study will measure the positive option of adoption of SMS gateway for both groups. Questionnaires will be used as research tools. Finally future research directions on SMS gateway adoption and usage will be discussed.

1.2 THE PROBLEM STATEMENT

Currently in Nairobi city, security incidents like terrorism attacks linked with Al shabaab, kidnappings, vehicle hijackings, burglaries, street muggings among others are on the increase. Civil unrests are now coming with some elements taking advantage of the demonstrations to loot or inflict injury. Also what needs to be considered is the mobility of various police officers in a police department who might be out in the field on patrol at the time of an incident occurrence. When urgent communication needs to be passed on in such cases using radio calls or memos it becomes a problem since the response time is increased due the time that such officers need in orders to dash to police stations or even relate to a radio call alert.

The police at the moment rely on the citizens reporting at the police desk at a police station in person to give input in the occurrence book (OB). Most of the public see this as hectic to them since some have to leave their busy schedules to go to the police stations for this exercise. The toll free 999 lines despite being brought back into service need manual intervention and recording to be done on various occurrences.

For security to be in place, we need to look into ways of improving the communication (information flow) between the police and the general public and also between the various police departments. Moreover the police might need to efficiently communicate with various security firms. This also needs to be put into thought.

There is need for a technological solution whereby the members of the public can pass urgent security related information to the police anytime without fear or inconvenience. The police on the other hand can push security updates or security information of concern to the citizens. We also need to ensure efficient and cheaper communication occurs within the police departments. For example SMS alerts broadcasted to all security officers about a stolen vehicle for search, new security threats in an area, suspicious terrorist figures tip off from the members of the public to the police etc. With such communication measures in place, both the police and the citizens will play a big role in enhancing security in an area since reported incidents can be acted upon as they are received and in a co-ordinated manner.

1.3 OBJECTIVES OF STUDY

1.3.1 General Objectives

The main objectives of this research are listed as follows:

i.   To study the current communication means used by the police and the general public, identify the gaps in the communication and if technologies like SMS gateway might be a solution for these gaps.

ii. To carry out the research on the limitations and challenges that might arise in the process of planning to implement and use an SMS gateway technology in the police setup for the purpose of security enhancement.

1.3.2   Specific objectives

The specific objectives will be:

i.   Setting up an SMS gateway and web-based portal for the gateway.

ii.   Conducting survey from the users on their perception with a positive notion of a possible adoption of the SMS gateway playing a role in an organization for the purpose of enhancing security.

1.4 SIGNIFICANCE OF STUDY

Since this is still a new area of research, it will contribute immensely to communication enhancement hence security enhancement within and outside police departments. The communication needs that can be attained through the usage of the SMS gateway include the following:

i.   Send security alert SMS to a single mobile phone.i.e. The communication controller can route a specific SMS to an individual police officer.

ii.   The communications controller can send a security SMS broadcast to a group of police officers for action on a certain issue of concern.

iii.   Different police groups can have their various private inbox where specific alerts are received from the public or from their seniors in matters of alert. E.g. inbox for patrol officers, traffic officers etc

iv.   A single incoming security alert SMS can be routed from a mobile phone to various police groups / departments for action.

This being current area of research will aid to clarify concepts and help other researchers to get more insights on the area of applying SMS technology to addressing security matters in a society. The proposed study will add knowledge to the current discussion on mobile computing SMS technology based systems.

1.5 THE SCOPE AND LIMITATIONS

This study will consider the integration of an SMS gateway and web-based portal. A GSM mobile phone which supports AT commands will be used as a modem.

A limited number of police officers and members of the public will be used in this study. The results of the usage by these users will only be generalized for other similar members.   Those who will participate in the study will do so voluntarily. The study will only be limited to some Nairobi City police stations / officers.

1.6 CONTRIBUTION TO STUDY

The proposed project will design and develop a prototype to enable testing of intra/inter police communication using SMS gateway by the users with the intention of giving a positive feedback which will form a basis of SMS gateway adoption for communication purposes with security enhancement in mind.

1.7 DEFINATION OF TERMS

Mobile Computing: is human–computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad-hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications

GSM: GSM (Global System for Mobile Communications, originally Groupe Spécial Mobile), is a standard set developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital cellular networks used by mobile phones. It became the de facto global standard for mobile communications.

SMS: Short Message Service (SMS) is a text messaging service component of phone, web, or mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between fixed line or mobile phone devices.

SMS Gateway: An SMS gateway is a telecommunications network facility for sending or receiving Short Message Service (SMS) transmissions to or from a telecommunications network that supports SMS. Most messages are eventually routed into the mobile phone networks. Many SMS gateways support media conversion from email and other formats.

VAS: A value-added service (VAS) is a popular telecommunications industry term for non-core services, or in short, all services beyond standard voice calls and fax transmissions. In the telecommunication industry, on a conceptual level, value-added services add value to the standard service offering, spurring the subscriber to use their phone more and allowing the operator to drive up their ARPU.

SS7: Signalling System No. 7 (SS7) is a set of telephony signalling protocols which are used to set up most of the world's public switched telephone network telephone calls. The main purpose is to set up and tear down telephone calls. Other uses include number translation, local number portability, prepaid billing mechanisms, short message service (SMS), and a variety of other mass market services.

SIM: A subscriber identity module or subscriber identification module (SIM) is an integrated circuit that securely stores the international mobile subscriber identity (IMSI) and the related key used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers).

SMSC: A short message service center (SMSC) is a network element in the mobile telephone network. Its purpose is to store, forward, convert and deliver SMS messages.

ESME: External Short Messaging Entity (ESME) is a term originally coined by Aldiscon to describe an external application that connects to an SMSC to engage in the sending and/or receiving of SMS messages.

MSC: The mobile switching centre server, abbreviated MSC Server or MSS, is a 3G core network element which controls the network switching subsystem elements.

HLR: The home location register (HLR) is a central database that contains details of each mobile phone subscriber that is authorized to use the GSM core network. There can be several logical, and physical, HLRs per public land mobile network (PLMN), though one international mobile subscriber identity (IMSI)/MSISDN pair can be associated with only one logical HLR (which can span several physical nodes) at a time. The HLRs store details of every SIM card issued by the mobile phone operator. Each SIM has a unique identifier called an IMSI which is the primary key to each HLR record.

VLR: The visitor location is a database of the subscribers who have roamed into the jurisdiction of the MSC (Mobile Switching Center) which it serves. Each main base station in the network is served by exactly one VLR, hence a subscriber cannot be present in more than one VLR at a time.

AT Commands: Many mobile and satellite transceiver units support the sending and receiving of SMS using an extended version of the Hayes command set, a specific command language originally developed for the Hayes Smartmodem 300-baud modem in 1977. The connection between the terminal equipment and the transceiver can be realized with a serial cable (e.g., USB), a Bluetooth link, an infrared link, etc. Common AT commands include AT+CMGS (send message), AT+CMSS (send message from storage), AT+CMGL (list messages) and AT+CMGR (read message).

Flash SMS: A Flash SMS is a type of SMS that appears directly on the main screen without user interaction and is not automatically stored in the inbox. It can be useful in emergencies such as a fire alarms or cases of confidentiality, as in delivering one-time passwords.

Intelligent Network (IN): The Intelligent Network (IN) is the standard network architecture specified in the ITU-T Q.1200 series recommendations. It is intended for fixed as well as mobile telecom networks. It allows operators to differentiate themselves by providing value-added services in addition to the standard telecom services such as PSTN, ISDN and GSM services on mobile phones.

PSTN: The public switched telephone network (PSTN) is the network of the world's public circuit-switched telephone networks. It consists of telephone lines, fiber optic cables, microwave transmission links, cellular networks, communications satellites, and undersea telephone cables, all inter-connected by switching centers, thus allowing any telephone in the world to communicate with any other. Originally a network of fixed-line analog telephone systems, the PSTN is now almost entirely digital in its core and includes mobile as well as fixed telephones

1.8 CHAPTER SUMMARY

The chapter begins by giving an overall of what an SMS and SMS gateway are and the common SMS applications.   The current problem of insecurity is highlighted. Due to this problem, the objects of the study are justified. Moreover, the significance and contribution of this study in mobile computing research for communication purposes is also discussed. Lastly, the scope and limitations of the study are also mentioned including the definitions of some of the terms in the study.

CHAPTER 2.0: LITERATURE REVIEW

2.1 THE POLICE ORGANIZATION AND COMMUNICATION MEANS
2.1.1 An Overview

With the new constitution (RPP, 2012) providing for sweeping reforms in the police, the Kenyan government had setup a new police system to reflect the changes. The goal of the police reform is to transform the police to a professional, efficient and accountable police service that is trusted by the public. The Ransley Report recommended the restructuring of the police services to include new organization, including the Police Service Commission (PSC) and the Independent Police Oversight Authority (IPOA).

The different police organizations carry out different functions, and re structured a little bit differently.

- **National Police Service (NPS):** works to maintain a safe and secure community; detecting, preventing and investigating crime; crime; maintenance of public order.

- **National Police Service Commission (NPS Commission)**: manages recruitment, employment, professional standards and discipline of the National Police Service.

- **Independent Police Oversight Authority (IPOA)**: investigates complaints made against the police, investigate all deaths in police custody, investigate matters that are not the subject of an individual complaint but that the IPOA think it should investigate, and make recommendations for action and report to parliament.

- **County Policing Authorities (CPAs)**: are also new bodies, established under the National Police Service Act. The CPAs are a key way for the local country community to be involved in the policy direction and strategy of the police in their own county. Community Policing Committees will also be established in each area.
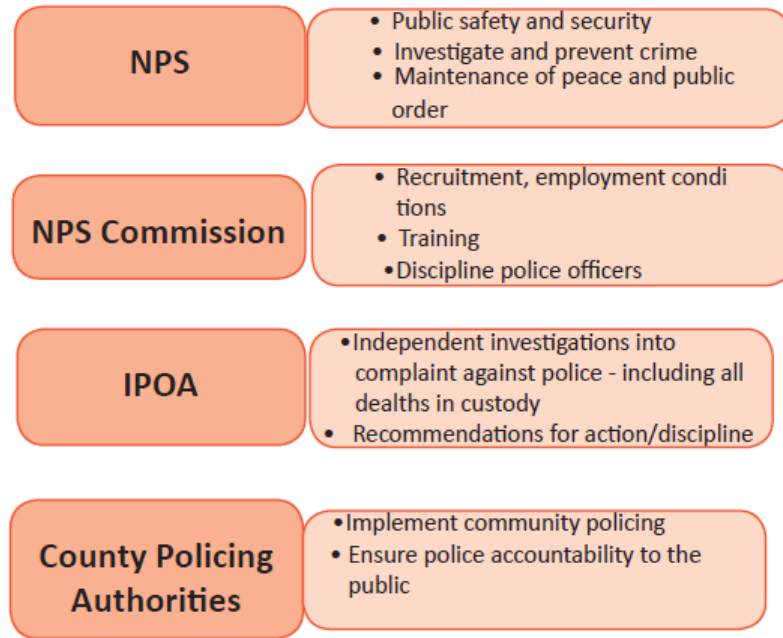
Figure 1 : The Police Service Organization (RPP, 2012)

2.1.2 The National Police Service (NPS)

The national police service is made up of:

- The Kenya Police service

- The Administration Police Service

- The Directorate of Criminal Investigation

The structure of reporting within NPS is as follows:
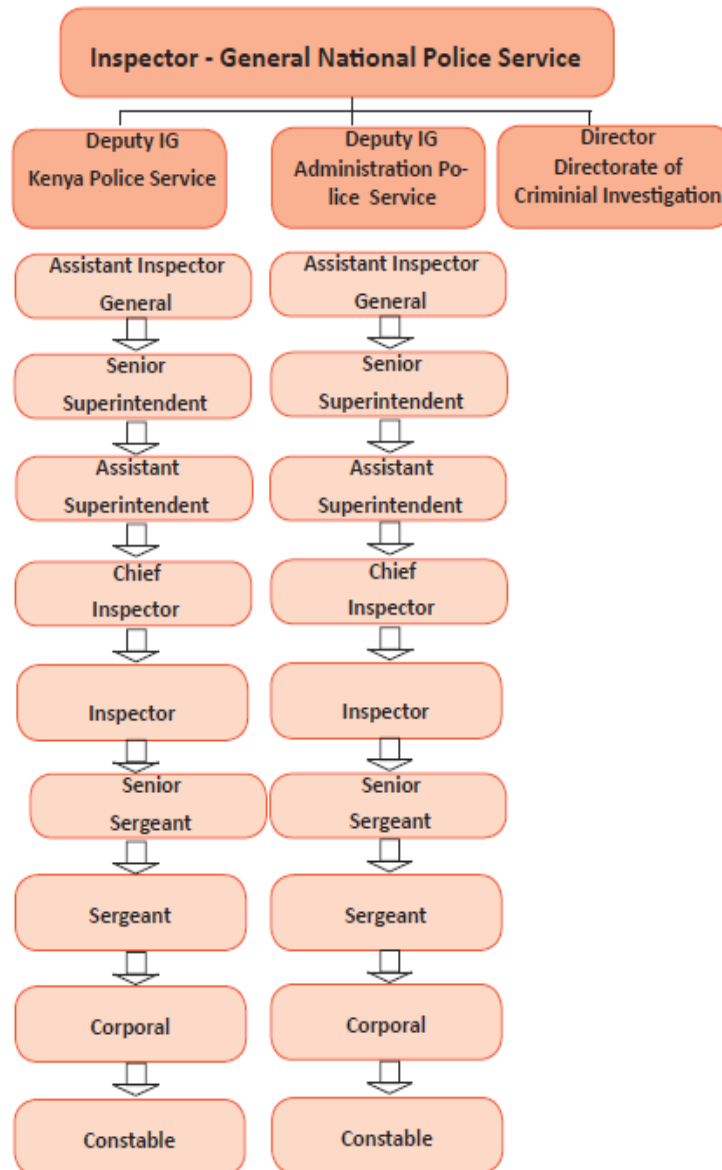
Figure 2 : The National Police Service structure (RPP, 2012)

2.1.3 The Police Communication means

The Kenyan police (2013) use High Frequency (HF) radios to communicate amongst themselves. For the communication between the police and the citizens, cell phones and fixed lines are used. In most cases, when a member of the public wants to tip off the police or make a complain, he or she is forced visit a nearest police station or post in order to do this.

In July 2013 (Standard Media, 2013), the Kenyan High court ordered the Communication Commission of Kenya (CCK), mobile phone service providers and the police service to restore the 999 emergency response numbers. This was after a case that was filed by a human rights activist. The Human rights activist had told the court that the nation was under the grip of insecurity and the toll free 999 police emergency response number was defunct. He argued that lack of emergency number amounts to police abdicating their duties to prevent and fight crime. Moreover when the police force is isolated from the public by not operating a toll free police emergency response number, then it is not operating efficiently, since for the police to succeed in their war against criminals, they need the active and effective participation of the general public in crime prevention.

According to Perry, D (2012). German police reportedly use a technology called silent SMS to track down crime suspects. According to a presentation given at the 28th Chaos Communication Congress in Berlin, Germany, 440,783 such "stealth" messages were sent by federal police authorities as well as the Bundesamt für Verfassungsschutz, Germany's equivalent of the FBI, in 2010. According to Heise Online, Germany's customs have picked up silent SMS as a tracking method, which is likely to result in a substantial increase in the use the technology. The customs alone sent 227,587 silent SMS in the first half of 2011. German authorities apparently use silent SMS to create a movement profile of suspects or locate their position. SMS pings are received by a cellphone, but the user will not be notified of it. However, the cellphone carrier will record the data in a log, which can be requested by the government. While the data do not provide information about the phone, they do deliver location data via the cell towers that were used when the silent SMS was sent.

Streicher (2010) managing director of BulkSMS.com, takes a look at SMS's role in preventing crime and enforcing the law.
From a crime prevention point of view, SMS is immensely powerful thanks to its ability to allow anonymous tip-offs. The Primedia Crime Line service, which was launched in June 2007 and offers an SMS tip-off line, has resulted in 941 arrests, and the recovery of more than R35.7 million's worth of stolen property, drugs and counterfeit goods. SMS also has the capacity to quickly and easily reach a large number of people on the move and is used effectively by the police force to co-ordinate and receive information from mobile volunteers, and also by neighbourhood watch schemes.

When it comes to law enforcement, SMS's are considered to be written documents according to the Electronic Communications and Transactions Act (ECT) and are admissible as evidence in both a criminal and civil court case. Just like an ordinary document would be assessed by the court to determine its integrity and evidential weight – for instance an original copy of a document with signatures would count more than a poor photocopy – SMS's are assessed based on their electronic details including when they were created, sent, modified or delivered.
From a practical point of view, SMS can also be very helpful in making the courts run smoothly. Simply by texting a witness the details of their court appearance and any delays can make the courts run more efficiently. Likewise

lawyers can use SMS to keep their clients up to date with lengthy legal processes.

British Police officers (Daily Mail, 2010) were being ordered to send texts rather than speak on their radios because of the sums charged by the firm that owns the police communications network. Police officers had been given a set of 16 numerical codes that correspond to buttons on their handset. By inputting the correct combination of digits, they could report their location and whether they were issuing a warrant, making an arrest, on a meal break or returning to base. The information was automatically fed into the control room computer. In an emergency, they could summon help in the normal way. But if they were involved in a routine procedure, they had been told to use the messaging facility instead. An investigation by The Mail found that forces across Britain had sent their staff on texting training courses. They included North Wales, Nottinghamshire, Cheshire, North Yorkshire, Kent, Hertfordshire, Durham, Hampshire, Norfolk, Dorset and Dyfed-Powys.

According to LAPD (2013), in response to demand from the public for secure and anonymous ways to submit crime tips to the authorities, the Los Angeles Police Department(LAPD) developed a new anonymous tip services for use by the public. Using 'Text-a-tip Service', User types "LAPD" plus their tip on their cell phone or PDA and texts it to "CRIMES" (274637). The text message is encrypted and an alias is generated, masking the identity of the sender from the police. The police have no way of determining the user's identity.

2.1   CRIME INCIDENTS IN NAIROBI CITY

2.1.1 An overview

Every day (SRIC, 2012), the mass media in Kenyan carries horrid episodes of wide-ranging criminal incidences. Typically, these incidences range from plain murders, carjacking-related shootings, robbery with violence, property break-ins, abductions, rape and defilement, muggings, armed livestock raids, and intimate partner violence – otherwise commonly referred to as domestic violence among other crimes.

Incidences of police officers being (literally) put on the firing line by hardened criminals have become all too common occurrences in the country. In fact, cases of armed violence indicate an increase in illegal arms in the country. For example, in the first ten months of 2010, the police were able to recover "… 128 rifles, 60 pistols, 10 toy pistols and 36,458 ammunitions in normal police operations."[2] These exclude 1,064 firearms and 3,078 ammunitions recovered from disarmament operation in the same period (SRIC, 2012).

As further stated by SRIC (2012), the plethora of criminal activities that are reported on a daily basis by both the print and electronic media channels in the country is simply mind-boggling: they are vicious and bizarre. For instance in February 2011, about 31,211 assorted ammunitions were recovered from a businessman's premises in Narok; and in June during an interdenominational prayer in Uhuru Park a devise exploded killing six people and injuring seventy two others.

The most unsettling reality is that criminal activities have now pervaded practically all facets of society in Kenya. Even hitherto serene and tranquil middle class neighbourhoods in urban centres are beginning to get alarmed by this deadly social vice. For example in February 2010, a Canadian national was kidnapped within International School of Kenya (was later rescued by police officers in Gatundu after fierce exchange of fire with the abductors) (SRIC, 2012).

Although efforts are being put in place to address the problem of crime, factors contributing to increase in crime such as proliferation of small arms and light weapons, presence of criminal gangs, inequitable distribution of resources, poor urban planning, unemployment and idleness among the youth, extreme poverty, drug and substance abuse, and ill preparedness of the police in terms of logistics and equipment, among other causes, are still far from being addressed (SRIC, 2012).

Indeed, the government is all too aware of the reality that safety and security is the fulcrum around which the country's potential for growth and prosperity rotate. In fact, the extent to which Vision 2030, as well as the UN Millennium Development Goals (MDGs) will be actualized depends to a large measure on the government's ability to create and sustain a stable and secure country. For instance, the reticence and reluctance that has been exhibited by foreign investors in the country has been rightly blamed on the oscillating security situation that continues to prevail in the country. Similarly, the highly progressive provisions as spelt out in the (new) Constitution can only be realized in an enabling atmosphere that is characterized by peace and tranquillity (SRIC, 2012).

As further articulated in the SRIC (2012) report, there is need to enhance an understanding of the nature, dynamics and index of crimes in the country through crime observatory. Amongst other benefits, crime observatory is important in analysing community safety, strengthening of the capacity for addressing the problem of youth and armed violence and more importantly monitoring and evaluating the impact of specific interventions targeted on crime prevention and management.

2.1.2 Police preparedness to combat crime

The National Accord signed in February 2008 (The Usalama Reforms Forum, 2012) recognized urgent implementation of Police Reforms as one of the items under 'Agenda 4'. Pursuant to commitment to implement Reforms, the Government appointed the National Task Force on Police Reforms to examine the institutional, policy, legislative and operational framework in which the Kenya Police and the Administration Police operated and make recommendations for comprehensive Reforms to transform the Police Services into professional and accountable security agencies that can effectively and efficiently deliver on their mandate.

Five critical Reforms areas and corresponding indicators under recommendations identified by the Report of the Commission of Inquiry into Post Election Violence 2008 and Report of the National Task Force on Police Reforms in 2010. These include:

(a) Restructuring the Police Services;

(b) Police accountability;

(c) Police management and human resource capacity;

(d) State of preparedness of the Police Services;

(e) Operational, tooling, logistical and technological capacity;

According to the Usalama Reforms Forum (2012) report, there has been some progress with the implementation of Reforms but not across the board. Of a total of 207 recommendations identified by the National Task Force on Police Reforms, 9 percent (18 recommendations) are on track with significant progress on implementation. Almost 50 percent (102 recommendations) are pending full implementation, albeit with serious challenges, 25 percent (52 recommendations) have had no significant action on them. 16 percent (35 recommendations) are stalled or blocked. Notable successes include the development and enactment of the National Police Service Act 2011, the National Police Service Commission Act 2011, and the Independent Policing Oversight Authority Act 2011. Other progress have been noted with the appointment of Policing Oversight Authority Board, the process to set up Internal Affairs Unit to provide for an internal mechanism to receive and investigate complaints against police by the public and police against police, development of Community Policing Policy guidelines and completion of a pilot project in Kikuyu Police Station to demonstrate best practice in Community Policing, development of a new Police Training Curriculum that extends the period of training from 9 to 15 months of basic training and additional 6 months cadet training for University graduate recruits.
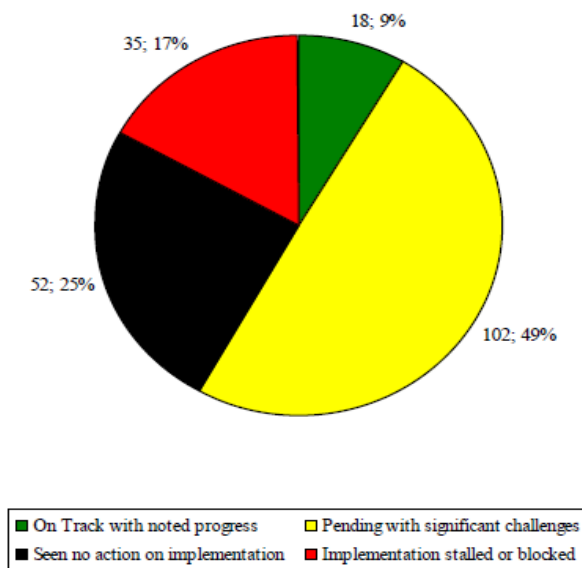
Figure 3 : Progress so far with implementation of police reforms (The Usalama Reforms Forum, 2012)

27

The Usalama Reforms Forum (2012) assessment concluded that although great lessons have been learnt following the 2007 post-election violence, the Police Services are no better prepared to address challenges posed by the terrorist groups and organized criminal gangs, to cope with crime and ever increasing security challenges characterizing the period preceding during and after the election than they were in 2007.

Of the five critical reform areas identified by the Report of the Commission of Inquiry into Post Election Violence 2008 and Report of the National Task Force on Police Reforms in 2010, the focus of this study will be on the Operational, tooling, logistical and technological capacity of the police force.

The police still lack necessary communication infrastructure, adequate vehicles, plan and equipment (The Usalama Reforms Forum, 2012). The visit to police stations observed that the police are yet to acquire and adopt modern policing technology. At the very basic level the police stations lacked computers, local radio with transfer connectivity capability, mobile phones, patrol dogs and tracker dogs, VHF radios.

2.1.3 Impact of reforms on challenges facing the police
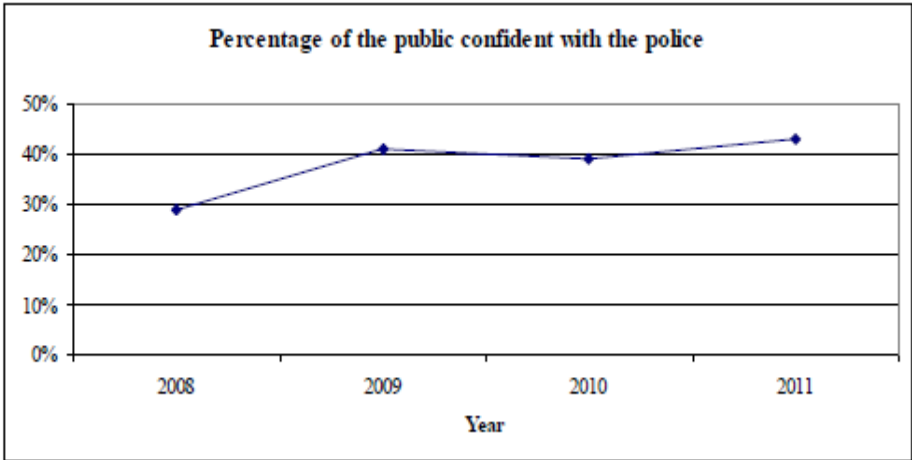
Figure 4 : Trust in the police (Kenya National Dialogue and Reconciliation (KNDR) Monitoring Project Review Report, 2012)
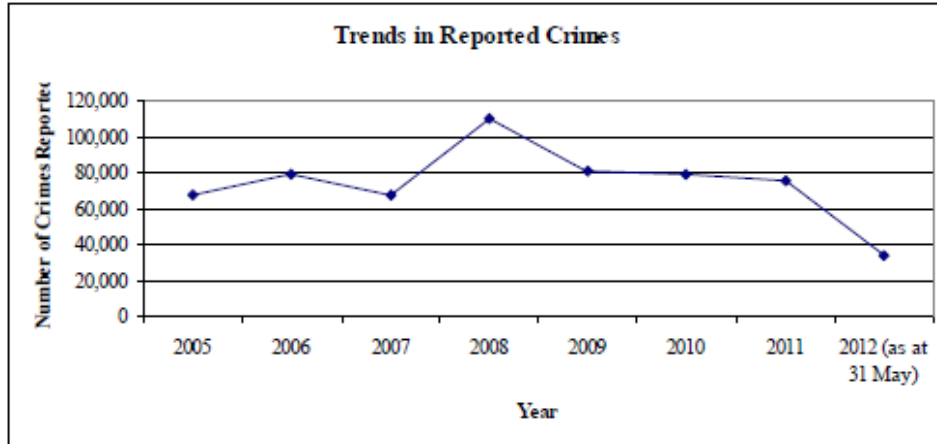
Figure 5 : Trends in reported crimes (The Usalama Reforms Forum, 2012)
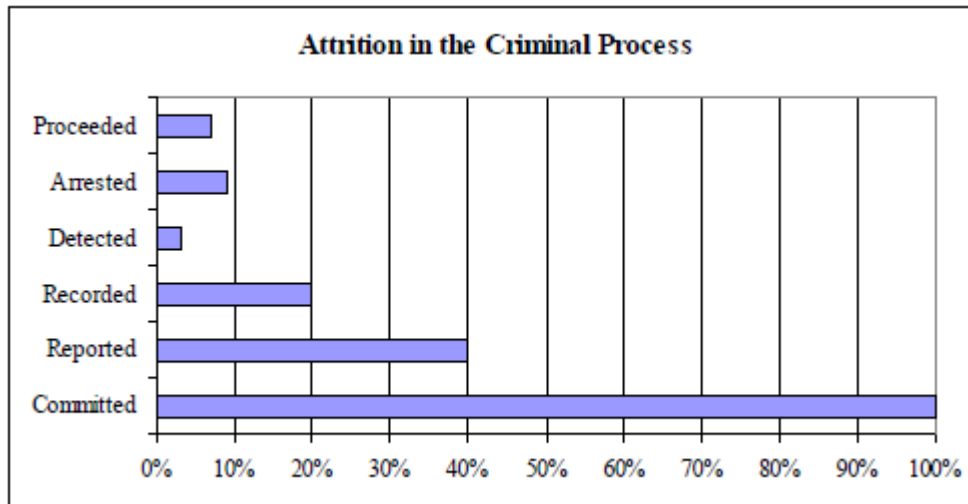
Figure 6 : Attrition in criminal process (The Usalama Reforms Forum, 2012)
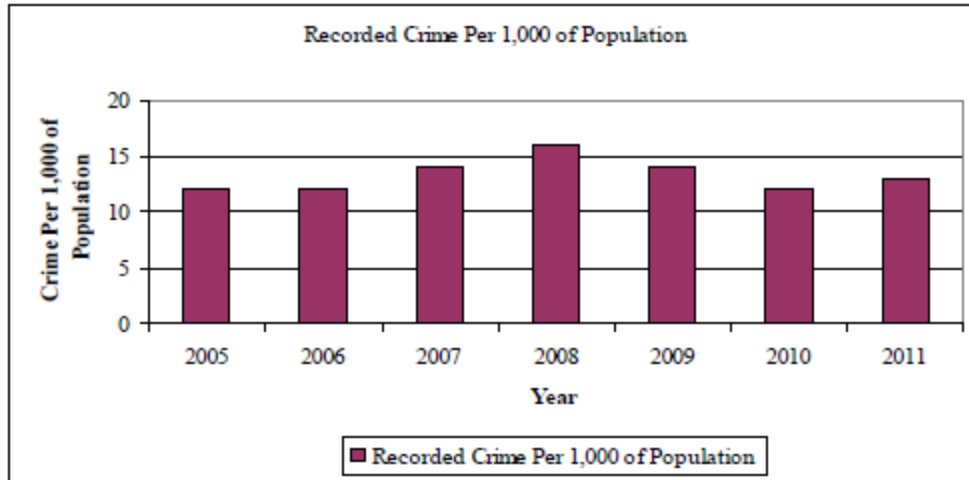
Figure 7 : Crime per 1,000 of population (The Usalama Reforms Forum, 2012)
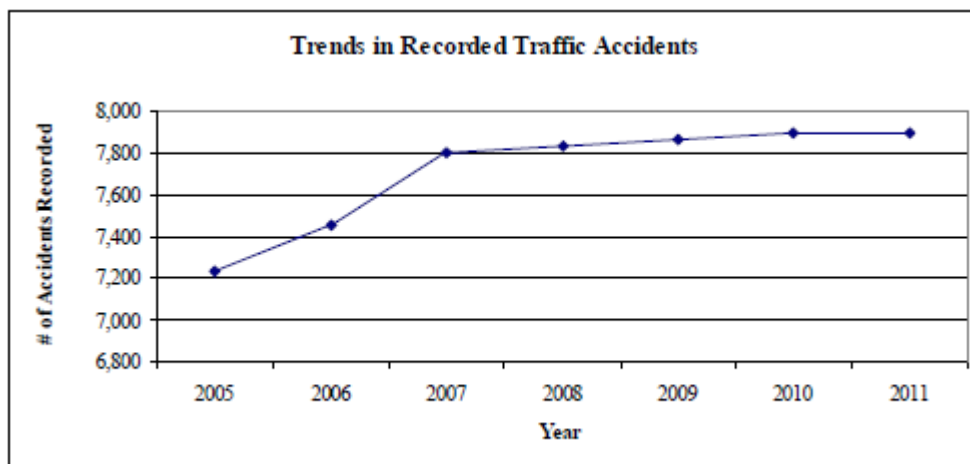
Figure 8 : Trends in recorded traffic accidents (The Usalama Reforms Forum, 2012)
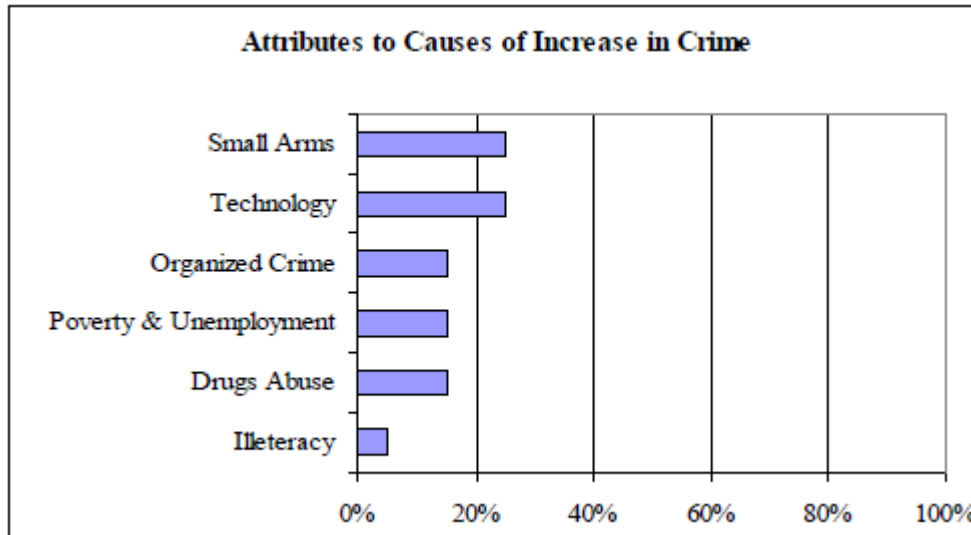
Figure 9 : Attributes to causes of increase in crime (The Usalama Reforms Forum, 2012)
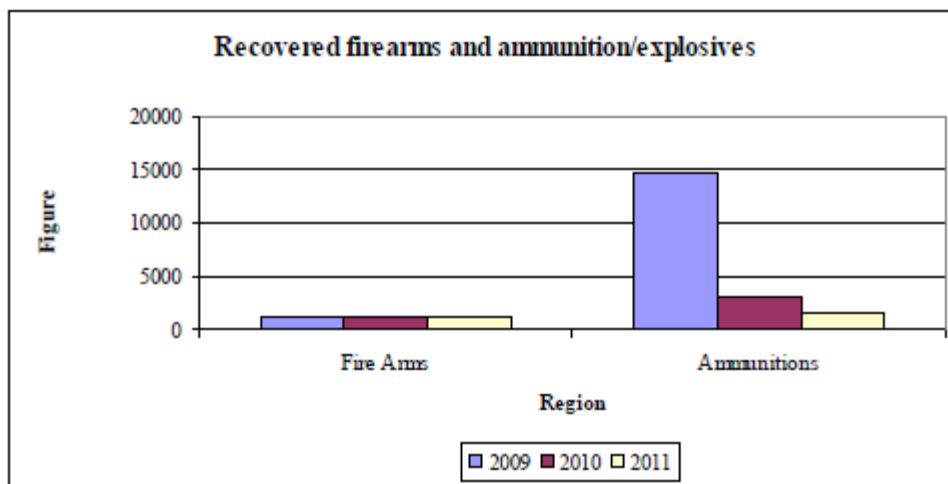
Figure 10 : Recovered firearms and explosives (The Usalama Reforms Forum, 2012)
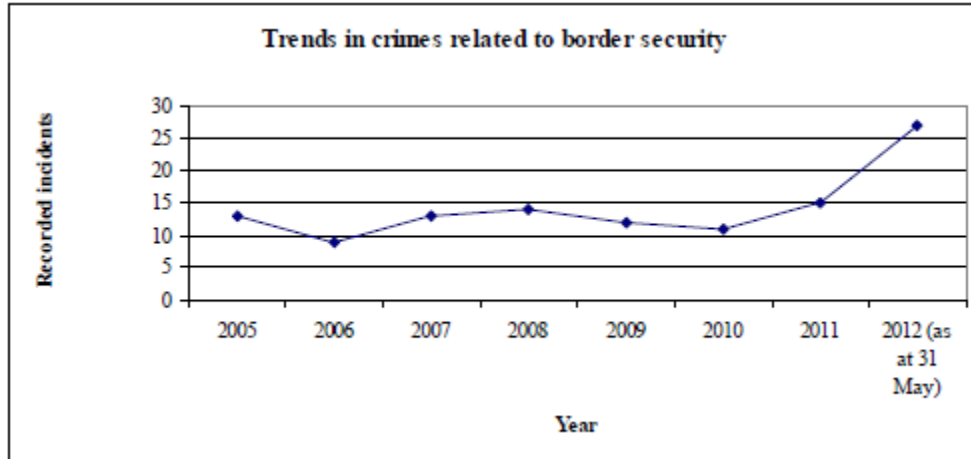
Figure 11 : Trends in crimes related to border security (The Usalama Reforms Forum, 2012)
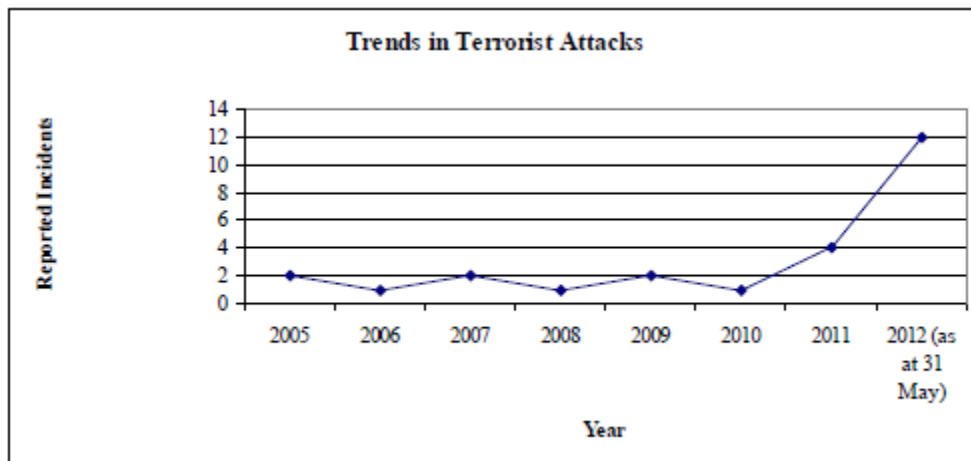
Figure 12 : Trends in Terrorist attacks (The Usalama Reforms Forum, 2012)

Number of Fatalities in Terrorist Attacks
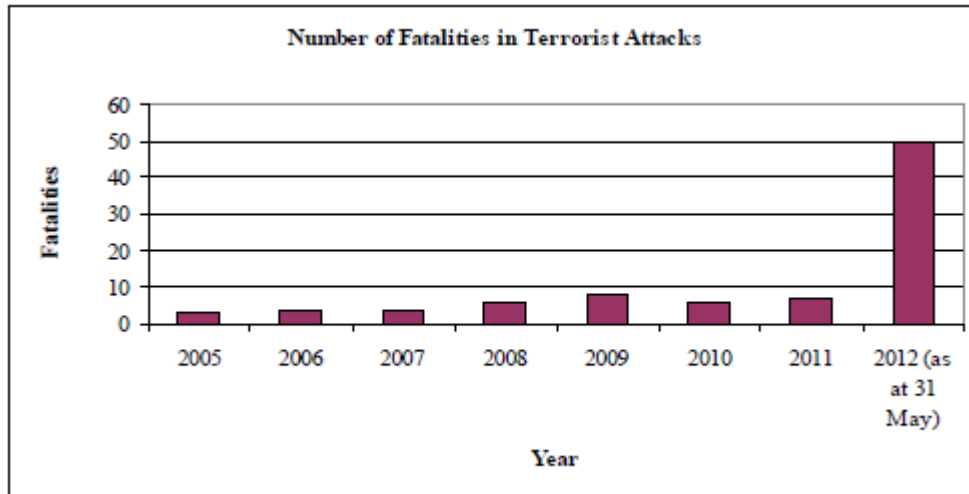
Figure 13 : Number of fatalities in terrorist attacks (The Usalama Reforms Forum, 2012)

How much respect would you say you have for the police?
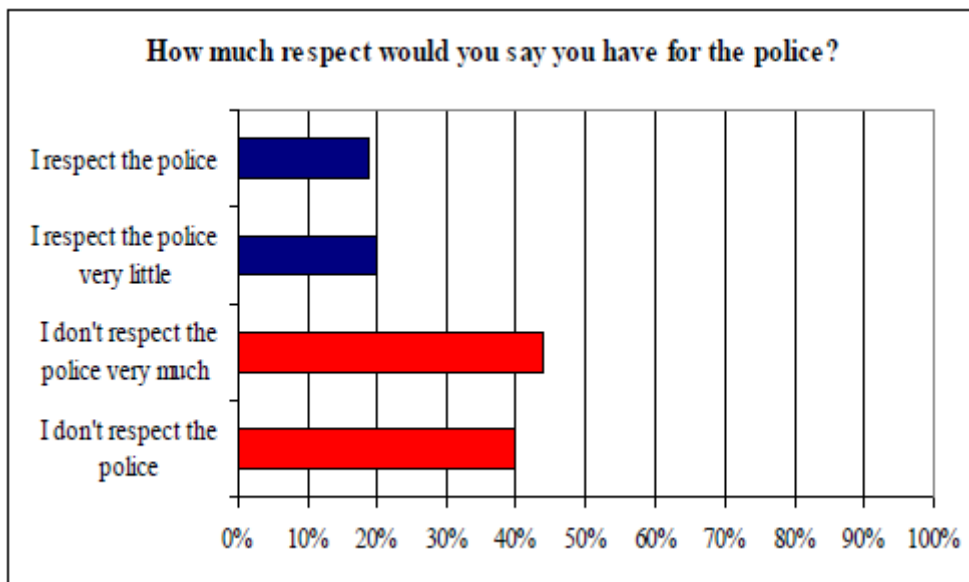
Figure 14 : Public Respect for the Police (The Usalama Reforms Forum, 2012)
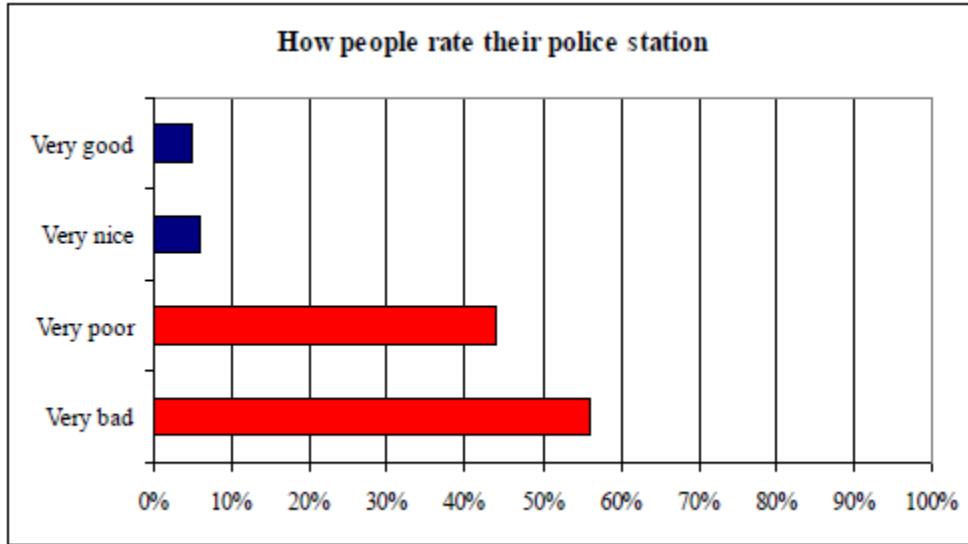
Figure 15 : How people rate their police stations (The Usalama Reforms Forum, 2012)
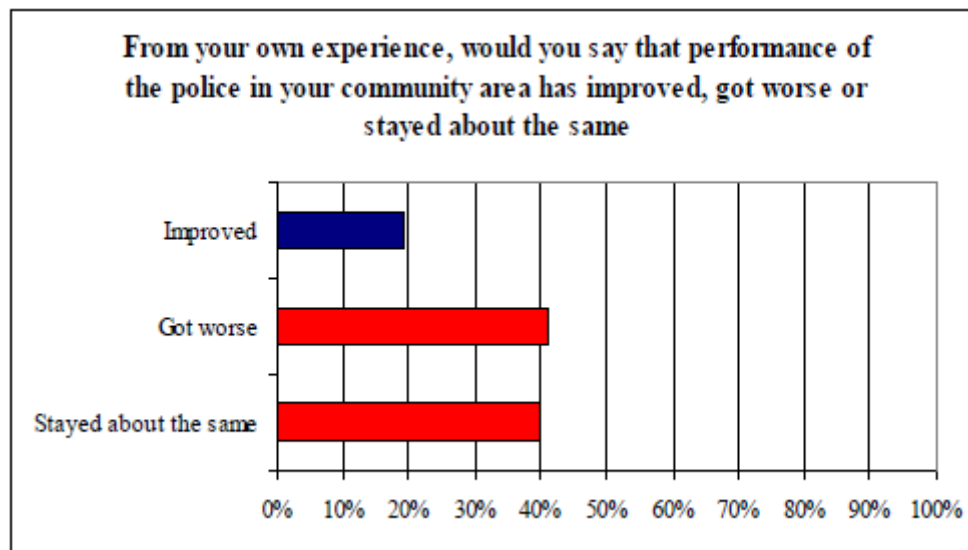
Figure 16 : Perception police performance (The Usalama Reforms Forum, 2012)

2.2   COMMUNITY POLICING

2.2.1 Definition of community based policing

Community Based Policing (CBP) is both a philosophy (a way of thinking) and an organization strategy (a way of carrying out the philosophy), that allows the police and the community to work together in new ways to solve problems of crime, disorder and safety issues to improve the quality of life for everyone in that community.

Recognising that communities are best placed to identify their own security and safety needs and how they can be met; communities must be actively involved in planning and implementing locally-defined solutions to their problems. Community members also play a key role in monitoring progress and providing feedback.

The following can be considered as the fundamental principles of CBP:

- practise policing by consent not coercion

- be part of the community not apart from it

- find out (together with the community) what the community's needs are

- work in partnership with other agencies and the public

- tailor the 'business' of policing to meet the community's needs

- be accountable for its 'business service'

- provide a quality service

2.2.2 Characteristics of community-based policing

The above principles can be translated into a set of characteristics of the police in a CBP paradigm. The police need to be:

- a service not a force

- accountable to the law and the public

- open and identifiable

- professional

- people-centred – including, for instance, sensitivities around gender, age, and group identities

- delivering a quality service – efficient and effective

- visible and accessible

- consultative and participative

- proactive

- preventative

2.2.3 Benefits of community-based Policing

This approach to CBP:

- Makes safety and security everybody's responsibility, not just that of the law enforcement agencies

- Enables the community to have a say in safety and security issues as they understand the issue

- Maximises resources within the community through shared responsibility and joint efforts

- Improves police accountability to the community by providing mechanisms for addressing complaints

- Mobilises the community to address pertinent issues beyond their immediate security, e.g. development

- Contributes to safer societies leading to enhanced economic development

- Encourages networking, constructive social relations and greater cohesion within the community

- Improves trust and confidence between community and the police

2.2.4 Piloting community-based policing at the local level

Since 2003, a variety of community-based policing projects and sites have been launched across Kenya. Two of these sites (Kibera and Isiolo) have largely been established and managed by Kenyan civil society partners. The lessons and experiences garnered in each site have subsequently been used to inform national thinking and practice on CBP. The type of activities carried out in each site has varied but has included: training and awareness-raising on CBP for police officers and communities, the establishment of Community Safety and Information Centres, support for practical projects, and anonymous information 'drop-in' boxes (Toa Habari kwa Polisi) posted across the two pilot sites in order to facilitate information exchange on community safety issues.

2.3   GSM NETWORK
2.3.1   <u>Global System for Mobile Communications (GSM)</u>

As explained by Talukder, Ahmed and Yavagal (2010), GSM is much more than just an acronym for Global System for Mobile Communication. It signifies an extremely successful technology and bearer for mobile communication system. GSM today covers 71% of all the digital wireless market. The mobile telephone has graduated from being a status symbol to a useful appliance. People use it not only in business but also in

personal life. Its principle use is for wireless telephony, and messaging through SMS. It also supports facsimile and data communication.

GSM is based on a set of standards, formulated in the early 1980s (See Table 1). In 1982, the Conference of European Posts and Telegraphs (CEPT) formed a study and developED a pan-European mobile system, which later rechristened as Global System for Mobile communication. The proposed GSM system had to meet certain objectives. These are:

- Support for international roaming.

- Good speech quality.

- Ability to support handheld terminals.

- Low terminal and service cost.

- Spectral efficiency.

- Support for a range of new services and facilities.

- ISDN capability.

Year	Event
1982	Groupe Special Mobile (GSM) established
1987	Essential elements of wireless transmission specified.
1989	GSM becomes an ETSI technical committee
1990	Phase 1 GSM 900 specification (designed 1987 through 1990) frozen
1991	First GSM network launched
1993	First roaming agreement came into effect
1994	Data transmission capability launched
1995	Phase 2 launched. Fax and SMS roaming services offered
2002	SMS volume crosses 24 billion/year, 750 million subscribers

Table 1: GSM history timeline (Talukder, Ahmed and Yavagal (2010))

Due to its innovative technologies and strengths, GSM rapidly became truly global. Many of the new standardization initiatives came from outside Europe. Depending on locally available frequency bands, different air interfaces were defined. Of these prominent ones are 900 MHz, 1800 MHz and 1900 MHz.

However, architecture, protocols, signalling and roaming are identical in all networks independent of the operating frequency bands.

GSM uses a combination of FDMA (Frequency Division Multiple Access) and TDMA (Time Division Multiple Access). The GSM system has an allocation of 50 MHz (890-915 MHz and 935-960 MHz) bandwidth in the 900 MHz frequency band. Using FDMA, this band it divided into 124 (125 channels, 1 not used) channels each with a carrier bandwidth of 200 KHz. Using TDMA, each of these channels is then further divided into eight time slots. Therefore with a combination of FDMA and TDMA we can realize a maximum of 992 channels transmitting and receiving. In order to be able to serve hundreds of thousands of users, the frequency must be re-used. This is done through cells.

The frequency re-use concept led to the development of cellular technology as originally conceived by AT&T and Bell Labs way back in 1947. The essential characteristics of this re-use are as follows:

- The area to be covered is subdivided into radio zones or cells (fig below). Though in reality these cells could be of any shape, for convenient modelling purposes these are modelled as hexagons. Base stations are positioned at the centre of these cells.

- Each cells i received a subset of frequencies fbi from the total set assigned to the respective mobile network. To avoid any time of co-channel interference, two neighbouring cells never use the same frequencies.

- Only at a distance of D (known as frequency re-use distance), the same frequency from the set fbi can be reused. Cells with distance D from cell i, can be assigned one or all the frequencies from the set fbi belonging to cell i.

- When moving from one cell to another during an on-going conversation, an automation channel change occurs. This phenomenon is called handover. Handover maintains an active speech and data connection over cell boundaries.

The regular repetition of frequencies in cells results in a clustering of cells. The clusters generated in this way can consume the whole frequency band. The size of a cluster is defined by k, the number of cells in the cluster. This also defines the frequency reuse distance D, figure below shows an example of a cluster size of 4.

2.3.2 GSM architecture

As further narrated by Talukder, Ahmed and Yavagal (2010), GSM networks are structured in a hierarchic fashion (see figure 1).
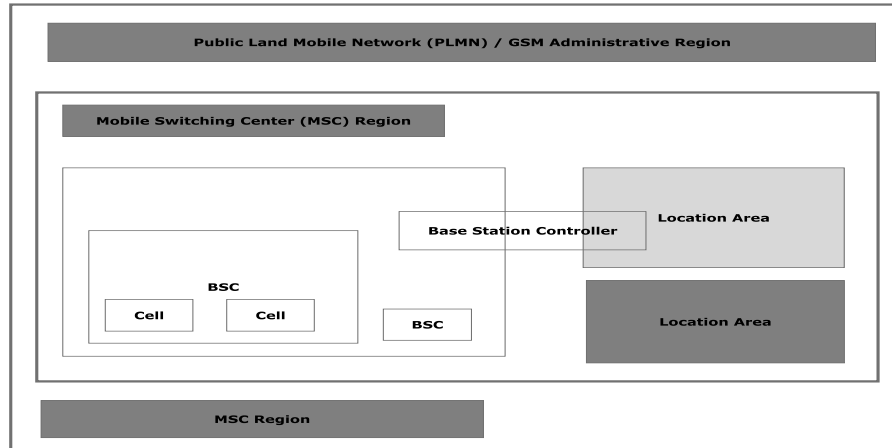
Figure 17 : GSM System Hierarchy (Talukder, Ahmed and Yavagal (2010))

It consists at the minimum one administrative region assigned to one MSC (Mobile Switching Centre). The administrative region is commonly known as PLMN (Public Land Mobile Network). Each administrative region is assigned is subdivided into one or many Location Area (LA). One LA consist of many cell groups. Each cell group is assigned to one BSC (Base Station Controller). For each LA there will be at least one BSC. Cells in one BSC can belong to different LAs.

Cells are formed by the radio areas covered by a BTS (Base Transceiver Station) (Fig 1). several BTSs are controlled by on BSC. Traffic from the MS (Mobile Station) is routed through MSC. Calls originating from or terminating in a fixed network or other mobile networks is handled by GMSC (Gateway MSC). Figure 2 below depicts the architecture of a GSM PLMN from technology point of view, whereas figure 3 depicts the same architecture from the operation point of view.
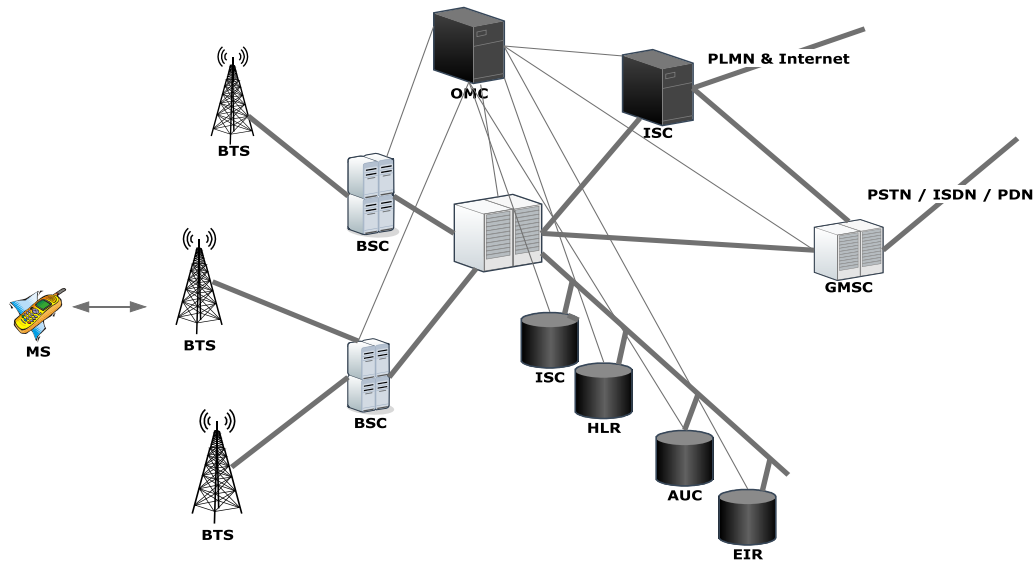
Figure 18 : Architecture of GSM (Talukder, Ahmed and Yavagal (2010))

For all subscribers registered with a cellular network operator, permanent data such as the service profile is stored in the Home Location Register (HLR). The data relate to the following information:

- Authentication information like International Mobile Subscriber Identity (IMSI).

- Identification information like name, address, etc., of the subscriber.

- Identification information like Mobile Subscriber ISDN etc.

- Billing information like prepaid or post-paid customer.

- Operator selected denial of service to a subscriber.

- Handling of supplementary services like CFU (Call Forwarding Unconditional), CFB (Call Forwarding Busy), CFNR (Call Forwarding Not Reachable) or CFNA (Call Forwarding Not Answered).

- Storage of SMS Service Centre (SC) number in case the mobile is not reachable so that whenever the mobile is connectable, a paging signal is sent to the SC.

- Provisioning information like whether long distance and international calls are allowed or not.

- Provisioning information like whether roaming is enabled or not.

- Information related to auxiliary services like voice mail, data, fax services etc.

40

- Information related to supplementary services like CLI (Caller Line Identification etc.).

- Information related to supplementary services for call routing. In GSM network, one can customize the personal profile to the extent that while the subscriber is roaming in a foreign PLMN, incoming calls can be barred. Also, outgoing international calls can be barred etc.

There is some variable information, which could be part of the HLR. This includes the pointer to the VLR, location area of the subscriber, power OFF status of the handset etc.

2.3.3 GSM entities

As clearly indicated by Talukder, Ahmed and Yavagal (2010), GSM technical specifications define different entities that form the GSM network by defining their functions and interface requirements. The GSM network can be divided into 5 main groups (fig 5.4):

- The Mobile Station (MS). This includes the Mobile Equipment and the Subscriber Identity Module (SIM).

- The Base Station Subsystem (BSS). This includes the Base Transceiver Station (BTS) and the Base Station Controller (BSC).

- The Network and Switching Subsystem (NSS). This includes Mobile Switching Centre (MSC), Home Location Register (HLR), Visitor Location Register (VLR), Equipment Identity Register (EIR), and the Authentication Centre (AUC).

- The Operation and Support Subsystem (OSS). This includes the Operation and Maintenance Centre (OMC).

- The data infrastructure that includes Public Switched Telephone Network (PSTN), Integrated System Digital Network (ISDN), and the Public Data Network (PDN).

2.3.3.1   Mobile Station (MS)

According to Talukder, Ahmed and Vagal (2010), Mobile station is a technical name of the mobile or the cellular phone. In early days mobile phones were a little bulk and some were even installed in cars like other equipment. Even the handheld terminals were quite big. Though the phones have become smaller and lighter, they are still called Mobile Stations. MS consists of two main elements:

- The mobile equipment or the mobile device. In other words, this a phone without the SIM card.

- The Subscriber Identity Module (SIM).

There are different types of terminals distinguished principally by their power and application. The handheld GSM terminals have experienced the highest evolution. The weight and volume of terminals are continuously decreasing.

The life of a battery between charging is also increasing. The evolution of technologies allowed decrease of power requirement to less than 1 W.

The SIM is installed in every GSM phone and identifies the terminal. Without the SIM card, the terminal is not operational. The SIM cards used in GSM phones are smart processor cards. These cards possess a processor and a small memory. By inserting the SIM card into the terminal, the user can have access to all the subscribed services. The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other security information. Another advantage of the SIM card is the mobility of the users. In fact the only element that personalized a terminal is the SIM card. Therefore, the user can have access to its subscribed services in any terminal using his or her SIM card. The SIM card may be protected against unauthorized use by a password or personal identity number. Typically, SIM cards contain 32 K bytes of memory. Part of the memory in the SIM card is available to the user for storing address book and SMS messages. Applications are developed and store in the SIM cards using SAT (SIM Application Toolkit). SAT is something similar to Assembly language of computers and is proprietary to the SIM vendor. Nowadays Java Smart cards are coming to the market. In Java Smart card, the applications are written in Java Language and are portable across SIM cards from different vendors.

2.3.3.2 <u>The Base station Subsystem</u> (BSS)

Talukder, Ahmed and Vagal (2010) further explain the BSS (Base Station Subsystem) as a system that connects the Mobile Station and the NSS (Network a d Switching Subsystem). It is in charge of the transmission and reception for the last mile. The BSS can be divided into two parts:

- The Base Transceiver Station (BTS) or the Base Station in short.

- The Base Station Controller (BSC).

The BTS corresponds to the transceivers and antennas used in each cell of the network. In a large urban area, a large number of BTSs are potentially deployed. A BTS is usually placed in the centre of a cell. Its transmitting power defines the size of a cell. The BTS houses the radio transmitter and the receivers that define a cell and handles the radio-link protocols with the Mobile Station. Each BTS has between one and 16 transceivers depending on the density of users in the cell.

BSC is the connection between the BTS and the Mobile Service Switching Centre (MSC). The BSC manages the radio resources for one or more BTSs. It handles handovers, radio-channel setup, and control of radio frequency power levels of the BTSs, exchange function, and frequency hopping.

2.3.3.3 <u>The Network and Switching Subsystem</u> (NSS)

According to Talukder, Ahmed and Vagal (2010), the central component of the Network Subsystem is the Mobile Switching Center (MSC). It does multiple functions. They are:

- It acts like a normal switching node for mobile subscribers for the same network (connection between mobile phone to mobile phone within the same network).

- It acts like a normal switching node for the PSTN fixed telephone (connection between mobile phone to fixed phone)..

- It acts like a normal switching node for ISDN.

- It provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, and handovers and call routing.

- It includes databases needed in order to store information to manage the mobility of a roaming subscriber.

These different services are provided in conjunction with several functional entities, which together form the Network Subsystem. The signalling between functional entities s in the network subsystem uses Signalling System Number 7 (SS7). SS7 is used for trunk signalling in ISDN and widely used in today's public networks. SS7 is also used for SMS, prepaid, roaming and other intelligent network functions.

The MSC together with Home Location Register (HLR) and Visitor Location Register (VLR) databases, provide call routing and roaming capabilities of GSM. The HLR is considered a very important database that stores information of subscribers belonging to the covering area of a MSC. Although a HLR may be implemented as a distributed database, there is a logically only one HLR per GSM network. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network. This includes information like current location of the mobile, all the service provisioning information and authentication data. When a phone is powered off, this information is stored in the HLR. The location of the mobile is typically in the form of the signalling address of the VLR associated with the mobile station. HLR is always fixed and stored in the home network, whereas the VLR logically moves with the subscriber.

The VLR can be considered a temporary copy of the important information stored in the HLR. VLR is similar to a cache, whereas HLR is the persistent storage. The VLR contains selected administrative information borrowerd from the HLR, necessary for call control and provisioning of the subscribed services. This is true for each mobile currently located in the geographical area controlled by a VLR. GSM standards define interfaces to HLR; however, there is no interface standard for VLR. Although each functionality entity can be implemented as an independent unit, all manufacturers of switching equipment implement VLR as an integral part of the MSC, so that the geographical area is controlled by the MSC corresponds to that controlled by the VLR.

Note: MSC contains no information about a particular mobile station – this information is stored in location registers.

When a subscriber enters the covering area of a new MSC, the VLR associated with this MSC will request information about the new subscriber from its corresponding HLR in the home network. For example, if a subscriber of a GSM network in Nairobi is roaming in Nakuru, the HLR data of the subscriber will remain in Nairobi with the home network, however, the VLR data will be copied to the roaming network in Nakuru. The VLR will then have enough information in order to assure the subscribed services without needed to refer to the HLR each time a communication is established. Though the visiting network in Nakuru will provide the services, the billing for the services will be done by the home network in Nairobi.

Within the NSS there is a component called Gateway MSC (GMSC) that is associated with the MSC. A gateway is a node interconnecting two networks. The GMSC is the interface between the mobile cellular network and the PSTN. It is in charge of routing calls from the fixed network towards a GSM user and vice versa. The GMSC is often implemented in the same node as the MSC. Like the GMSC, there is another node called GIWU (GSM Interworking Unit). The GIWU corresponds to an interface to various networks for data communications. During these communications, the transmission of speech and data can be alternated.

2.3.3.4   The Operation and Support Subsystem (OSS)

Talukder, Ahmed and Vagal (2010) define OSS as what controls and monitors the GSM system. The OSS is connected to different components of the NSS and to the BSC. It is also in charge of controlling the traffic load of the BSS. However, the increasing number of base stations, due to the development of cellular radio network, has resulted in some of the maintenance tasks being transferred to the BTS. This transfer decreases considerably the costs of maintenance of the system. Provisioning information for different services is managed by this subsystem.

Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment within the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). EIR contains a list of all valid terminals. An IMEI is marked as invalid if it has been reported stolen or it is not type approved. The EIR allows the MSC to forbid calls from this or unauthorized terminals.

Authentication Centre (AUC) is responsible for the authentication of a subscriber. This is a protected database and stores a copy of the secret key in each subscriber's SIM card. These data will help to verify the user's identity.

2.3.3.5   Message Center

According to Talukder, Ahmed and Vagal (2010), SMS is the most popular data bearer / service within GSM with an average of one billion SMS messages (at the end of 2002) transacted everyday around the world, with a growth of an average half a billion every month. The SS7 signalling channels are always physical present but mostly unused, be it in during an active user connection or in the idle state. It is therefore, quite an attractive proposition to use these channels for transmission of used data. SMS uses the free capacity of the signalling channel. Each SMS message is made up of 160 characters in length when 7-bit English characters are used. It is 140 octets when 8-bit

characetrs (some European alphabets) are used, and 70 characters in length when non Latin alphabets such as Arabic, Chinese or Hindi are used (70 characters of 16 bit Unicode). SMS is a proactive bearer and is always ON network. Message centre is also serviced to a as Service Centre (SC) or SMS Controller (SMSC). SMSC is a system within the core GSM network, which works as a store and forward system for SMS messages. Refer to figure 5.5 for SMS architecture.

2.4   MOBILE SERVICE ARCHITECTURES

2.4.1 <u>Voice communication</u>

As indicated by its name, the objective of mobile telecommunications systems is to provide communication between mobile distant persons. These systems only supported direct voice communication or telephony between two participants, but supplementary services like call forwarding, barring and voice mail were added later on. The mobile telephony service is realized by components called Mobile Station (MS) and on the mobile network. On the MS, there are components both on the Mobile Equipment (ME) and on the subscriber Identity Module (SIM). To establish a telephone conversation the service components on the MS are collaborating with the ones on the mobile network to allocate a channel and to maintain it throughout the session even when the MS is moving and changing base stations. The components on the mobile phone are installed by the manufacturer while the ones on the network are delivered by network suppliers (Zareen et al, 2011).

2.4.2 <u>Supplementary services within Intelligent Network</u>

It does not take long time before there is a need for more advanced call control services like call forwarding, barring, voice mail, premium call, etc. As shown in Figure 3 an IN (Intelligent Network) Service Control Point (SCP) is introduced in the mobile network to allow the implementation of supplementary services. It is worth mentioning that these services are derivatives centered on the voice communication service. Another restriction is that the SCP is implemented on equipment manufacturer proprietary technologies. The SCP is also located inside the telecom operator domain making third party service development difficult (Zareen et al, 2011).
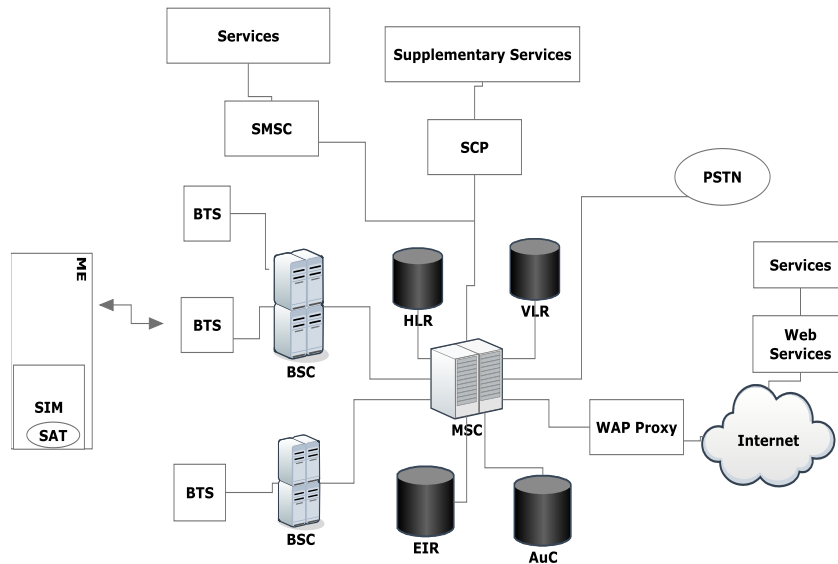
Figure 19 : Enabling Services with Intelligent Network (Zareen et al, 2011)

2.4.3 Enabling Services with Intelligent Network

The telecom operators want to have other services than telephony and its derivatives and turn to the SIM, which are their property. Unfortunately, although the SIM is a smart card having both processing and storage capabilities necessary for new services. The SIM is supposed to be the slave executing orders from its master, the ME. To remedy this, the SIM Application Tool-kit (SAT) is introduced to allow applications/services residing on the SIM to control the input and output units. With SAT it is possible to develop applications on the SIM but there are many restrictions. First SAT applications should be small in size. Secondly, the installation of applications on the SIM is controlled by operators who are reluctant to open the access due to security(Zareen et al, 2011).

2.4.4 Text services with Short Message Service (SMS)

SMS-C is responsible to store and forward messages to and from mobile phone (see figure 3). In the illustration, components used for SMS are the client in the ME advanced SMS services are implemented by Perl scripts. Provisioning of SMS services requires installation of the above mentioned application on an SMS Gateway the system running the SMS Gateway to act as an SMSC itself (e.g. a PC using a radio modem through a serial port or USB port). To have direct access to an SMSC requires cooperation with the operator that owns the SMSC, which often can provide a TCP connection for sending/receiving SMS messages part of a service. The advantage of the above solution is that to receive revenue from generated traffic. The problem with access to SMS services is remembering both the service access number and the additional identifiers and parameters for a specific service (the protocol) (Zareen et al, 2011).

2.4.5 Internet Access with WAP

Wireless Application Protocol (WAP) was to provide access to the WWW on handheld terminals. A micro browser installed in the Mobile Equipment is communicating with a WAP Proxy introduced between the Internet and the mobile network to convert Internet protocols to Wireless binary protocols as shown in figure 3. On the terminal side, a WAP browser is located in the ME and services are connected to a Web server on the network side. Development of WAP services can be performed by programming experience. Most services typically consist of some static WML content together with a CGI-script as back-end that can generate dynamic content retrieved from for example other Web sites or from a DBMS. One restriction of the technology is that it is not possible to access ordinary WebPages using a WAP browser (Zareen et al, 2011).

2.5   *SMS NETWORK ARCHITECTURE*
2.5.1 Short Messaging Service (SMS)

According to Kaur et al (2012), SMS (Short Message Service), commonly referred to as "text messaging," is a service for sending short messages of up to 160 characters (224 characters if using a 5-bit mode) to mobile devices, including cellular phones, smartphones and PDAs. SMS is similar to paging. However, SMS messages do not require the mobile phone to be active and within range and will be held for a number of days until the phone is active and within range. SMS messages are transmitted within the same cell or to anyone with roaming service capability. They can also be sent to digital phones in a number of other ways, including:

    i.   From one digital phone to another

    ii.   From Web-based applications within a Web browser

    iii.   From VoIP applications like Skype

    iv.   From some unified communications applications.

Typical uses of SMS include:

    i.   Notifying a mobile phone owner of a voicemail message

    ii.   Notifying a salesperson of an inquiry and contact to call

    iii.   Notifying a doctor of a patient with an emergency problem

    iv.   Notifying a service person of the time and place of their next call

    v.   Notifying a driver of the address of the next pickup

Enhanced messaging service (EMS), an adaptation of SMS that allows users to send and receive ringtones and operator logos, as well as combinations of simple media to and from EMS compliant handsets. Many of these uses depend upon short telephone numbers called Common Short Codes (CSCs), usually consisting of five digits, that are used to address SMS and MMS messages from cellular telephones. In recent years, SMS spam has become an issue

for some users a security attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto a cellular phone or other mobile device. Users can send messages from a computer via an SMS gateway. SMS gateways are Web sites that allow users to send messages to people within the cell served by that gateway. They also serve as international gateways for users with roaming capability (Kaur et al, 2012).

2.5.2 SMS Network Layers

In GSM network, SMS has four layers:

   i.   SM-AL (Application Layer)

   ii.   SM-TL (Transfer Layer)

   iii. SM-LL (Lower Layer)

   iv.   SM-RL (Relay Layer)

SMS gateways are located in the SM-AL layer. When an SMS is being sent, the software creates a protocol data units transported by the SM-TL layer. When a GSM device attached to the PC receives an SMS message, the message is encoded according to the SM-TL layer PDU specification. An SMS gateway decodes this PDU and makes the message readable for computer programs and computer users.
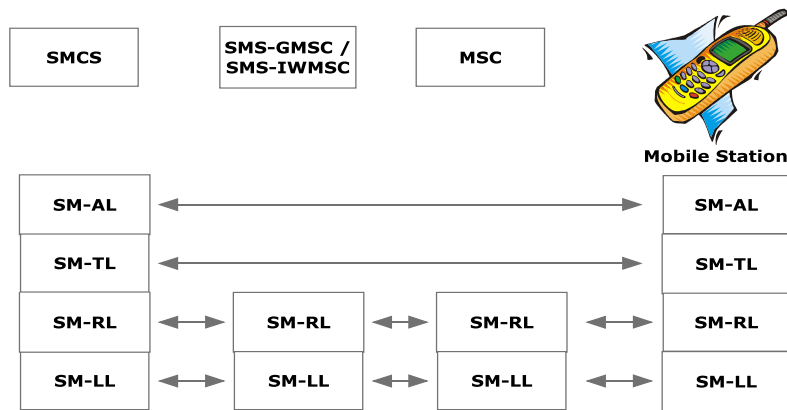
Figure 20 : SMS network layers (Kaur et al, 2012)

2.5.3 SMS Network Architecture

There are two types of SMS according to Talukder, Ahmed and Vagal (2010), SM MT (Short Message Mobile Terminated Point-to-Point), and SM MO (Short Message Originated Point-to-Point). SM MT is an incoming short message from the network and is terminated in the MS (phone or mobile station). SM MO is an outgoing message, originated in the MS, and forwarded to the network for delivery. For an outgoing message, the SMS is sent from the phone to SC via the VLR and the interworking MSC (IWMSC). For incoming SMS message, the path is from SC to the MS via the HLR and the Gateway MSC (GMSC). See figure 5.

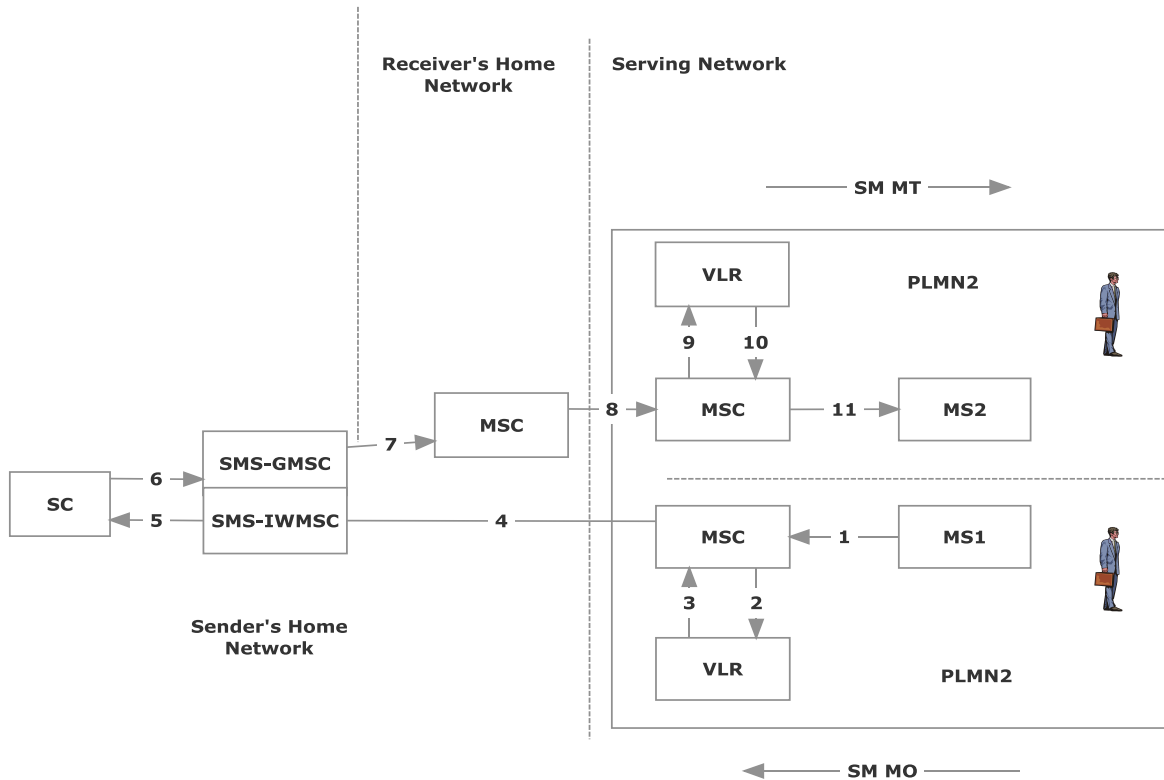Figure 21 : Flow of SMS between two MS (Talukder, Ahmed and Yavagal (2010))

To use SMS as a bearer for information exchange, the origin server or the Enterprise server needs to be connected to the SC through a shory message entity (SME) as in figure 6. The SME in this case works as an SMS gateway, which interacts to the SC in one side, and the enterprise server on the other side.

2.6   SHORT MESSAGE MOBILE TERMINATED (SM MT)

For an SM MT message, the message is send from SC to the MS. This whole process is done in one transaction (figure 6). For the delivery of MT or incoming SMS messages, the SC of the serving network is never used. This implies that an SMS message can be sent from any SC in any network to a GSM phone anywhere in the world. This makes any SM MT message mobile operator independent (Talukder, Ahmed and Yavagal (2010).
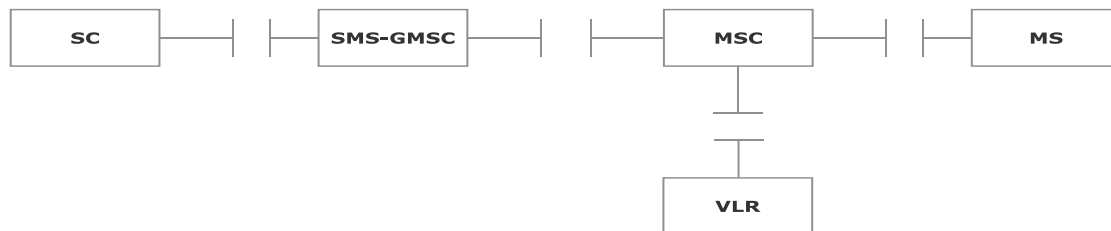

Figure 22 : Interface Involved in the SM MT Procedure (Talukder, Ahmed and Yavagal (2010))

49

2.7   SHORT MESSAGE MOBILE ORIGINATED (SM MO)

SM MO is an outgoing message originated in the MS where generally the user types in a message and sends it to another MSISDN number or application. For an MO message, the MSC forwards the message to the home SC of the sender. The SC is an independent computer in the network and works as a store and forward node with a large database.   The database is used to store the SMSs. In SS7 terminology SC is an SCP (Service Control Point) within the SS7 cloud. MO message works in two asynchronous phases. In the first phase, the message is sent from the MS to the home SC as an MO message (figure 7). In the second phase, the message is sent from the home SC to the receiving MS as an MT message (figure 6). It is possible to attempt to send an SMS message to an invalid MSISDN number. In such a case, the message will be sent successfully from the MS to the SC. However, it will fail during the SC to the MS transfer. The user will see SM MO message sent successfully but SM MT message delivery will fail (Talukder, Ahmed and Yavagal (2010).
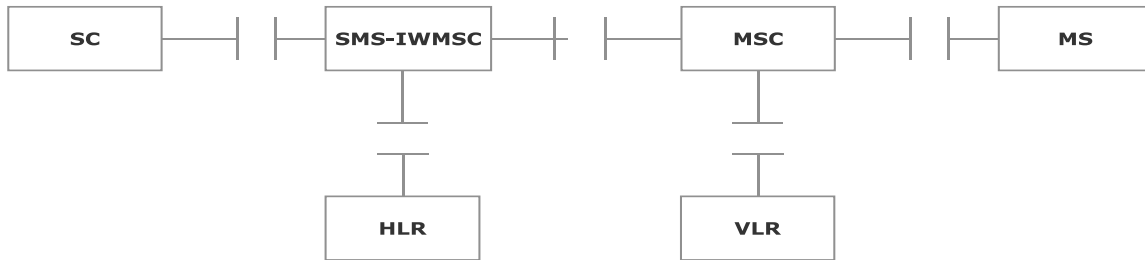
Figure 23 : Interface Involved in the SM MO Procedure (Talukder, Ahmed and Yavagal (2010))

2.8   SMS AS AN INFORMATION BEARER

According to Talukder, Ahmed and Yavagal (2010)), SMS is a very popular bearer in the person-to-person, mobile-to-mobile or point to point messaging domain. However, it is gaining popularity in other verticals like enterprise applications, services provided by independent service providers as ASP (Application Service Provider), and notification services, where one endpoint is a mobile phone but the other end point is a mobile application. Here SMS functions as an input-output media for information exchange for mobile application (figure 8).
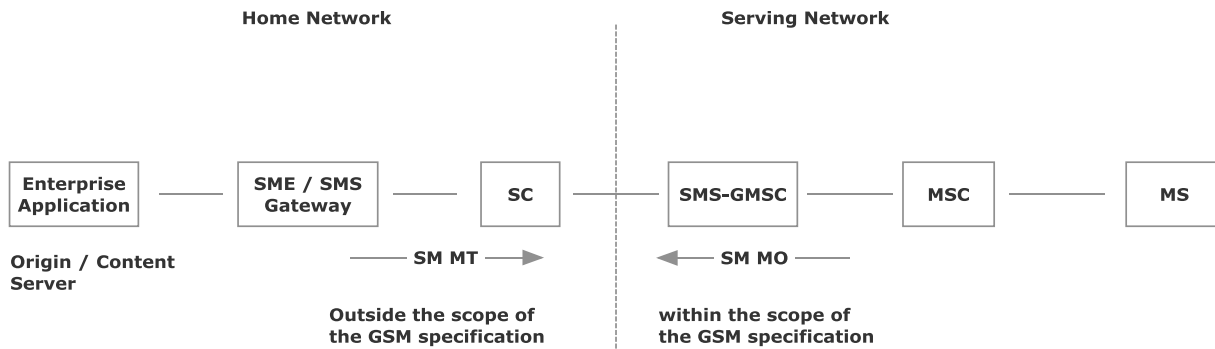
Figure 24 : SMS as an Information Bearer / Medium for Mobile Application (Talukder, Ahmed and Yavagal (2010))

50

2.9 PROPOSED MODEL FOR SECURITY ENHANCEMENT VIA AN SMS GATEWAY

The SMS gateway web interface will be accessed by the authorized police officers in a station mostly using mobile based web interfaces or from their desktop PCs at the station.
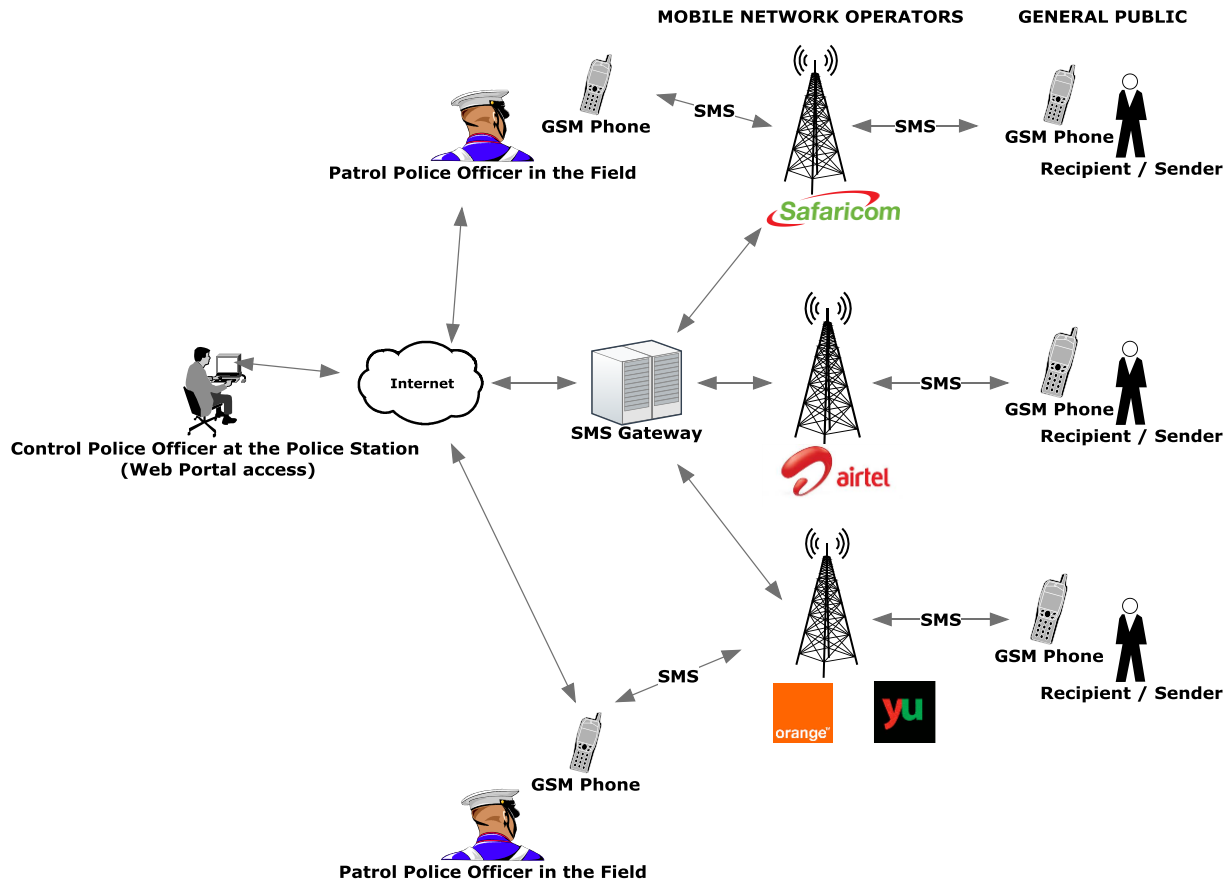
Figure 25: Proposed Police Security Enhancement model via SMS Gateway

Using the proposed model, the communication of both the police at the control and in the field can enriched in the following ways:

i.   They can send security alert SMS to a single mobile phone e.g. the communication controller can route a specific SMS to an individual police officer.

ii. They can send a security SMS broadcast to a group of police officers for action on a certain issue of concern.

iii. Various Police groups can have their various private inbox where specific alerts are received from the public or from their seniors in matters of alert. E.g. inbox for patrol officers, traffic officers etc

iv.   A single incoming security alert SMS can be routed from a mobile phone to various police groups / departments for action.

This is highlighted by the below functional model of this proposed model:

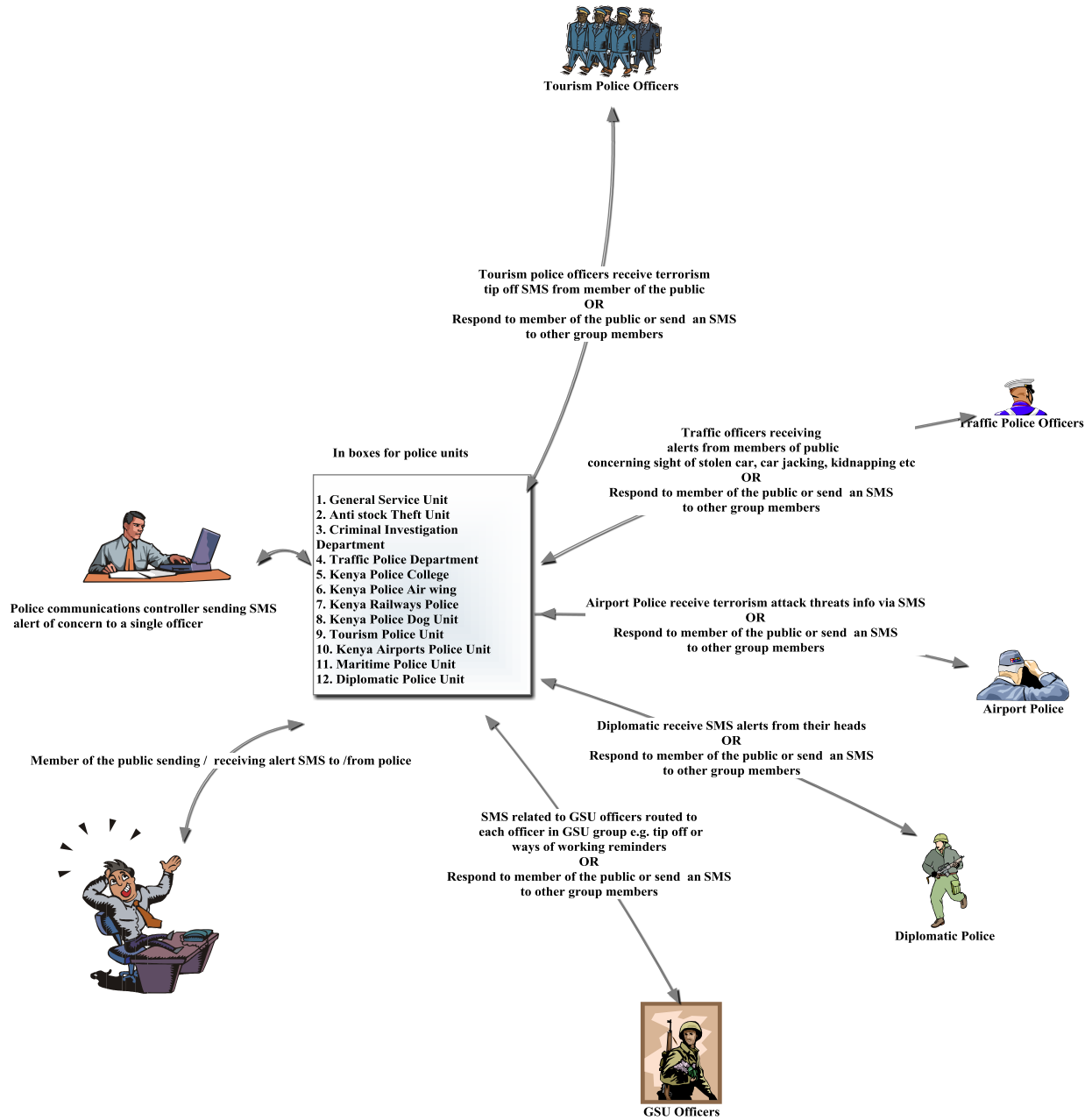**Tourism Police Officers**

Tourism police officers receive terrorism
tip off SMS from member of the public
OR
Respond to member of the public or send an SMS
to other group members

Traffic Police Officers

Traffic officers receiving
alerts from members of public
concerning sight of stolen car, car jacking, kidnapping etc
OR
Respond to member of the public or send an SMS
to other group members

In boxes for police units

1. General Service Unit
2. Anti stock Theft Unit
3. Criminal Investigation Department
4. Traffic Police Department
5. Kenya Police College
6. Kenya Police Air wing
7. Kenya Railways Police
8. Kenya Police Dog Unit
9. Tourism Police Unit
10. Kenya Airports Police Unit
11. Maritime Police Unit
12. Diplomatic Police Unit

Airport Police receive terrorism attack threats info via SMS
OR
Respond to member of the public or send an SMS
to other group members

Airport Police

Police communications controller sending SMS
alert of concern to a single officer

Diplomatic receive SMS alerts from their heads
OR
Respond to member of the public or send an SMS
to other group members

Member of the public sending / receiving alert SMS to /from police

SMS related to GSU officers routed to
each officer in GSU group e.g. tip off or
ways of working reminders
OR
Respond to member of the public or send an SMS
to other group members

Diplomatic Police

GSU Officers

Figure 26 - Nairobi police SMS Gateway Functional Model

2.10 CHAPTER SUMMARY

This chapter provides a more detailed description of literature published in the study area. The main areas discussed are: security status in Nairobi, community policing concept, GSM network, mobile service architectures, SMS network architecture, SM MT, SM MO and SMS as an information bearer. The chapter ends with a description of the proposed model for enhancing security within and outside the police force via the usage of an SMS gateway. A functional model to illustrate how the proposed model can be used is also illustrated.

CHAPTER 3.0 METHODOLOGY

This study will be carried out in two phases the first part will be system analysis and configurations and the second part will be involve carrying out the survey among the members of the public and the police.

System analysis and configurations

This phase will include three main tasks: the development of the SMS gateway, configuration and setup of web based portal.

The SMS gateway backend will be developed using Kannel. This gateway will be talking to many different SMS centers (SMSC) of mobile operators. The web based portal will be deployed using playSMS and MySQL. The police will login to the SMS gateway using their user name and password in order to send or receive SMS alerts.

The SMS gateway and the web based portal will be installed on Linux Fedora 20. Kannel is an open source SMS gateway software. The kannel source code will be compiled and installed on Linux Fedora. The setup will first be tested before it is deployed to be used by police officers / general public.

Police officers & members of the public survey

This will be second phase after the SMS gateway has been deployed and running. Police officers and members of the public in Nairobi will be invited to use the gateway. The police officers will be from some police stations. Those who will participate in this study will do so voluntarily.

Once they have used the SMS gateway they will be expected to fill questionnaire on their view of passing of information to and from police officers (or general public) using their mobile phones. The mobile phones that will be used in this study will be any mobile device and does not need to be a smartphone.

3.1 RESEARCH DESIGN

This study will utilize the descriptive method using both qualitative and quantitative approaches in order to gather the necessary data. Qualitative research has a primary advantage since it is more open to the adjusting and refining of research ideas as an inquiry proceeds. Moreover, the researcher does not attempt to manipulate the research setting, as in an experimental study, but rather seeks to understand naturally occurring phenomenon in their naturally states. On the other hand, quantitative method is compatible with the study because it allows the research problem

to be conducted in a very specific and set terms besides, quantitative research plainly and distinctively specifies both the independent and the dependent variables under investigation.

For this study, primary research and secondary research will be used. Primary research will be conducted using questionnaire which will be given to the police officers and selected general public to participate in this study. The questions that the police officers / member of the public will be asked will be on perception of SMS gateway as a communication gateway for enhancing security. Here the questionnaires will be used to collect quantitative data and the interviews will be used to provide qualitative insights into the data collected. The secondary data will be based from the recent literatures published sources this includes bibliographic databases, journals and conference proceedings.

3.2 DATA COLLECTION

3.2.1 Sample Population

In this study, stratified random sampling procedure will be used. There will be two groups of which the strata will be drawn ie. One group will be drawn from members of the public using simple random sampling method the other strata will be police officers which the remaining participants will be drawn. The sampling frame of this study will involve 67 members of the public and police officers from various police departments who have mobile phones and who have used web browser before.

3.2.2 Instruments

The main instrument for collecting data will be questionnaires. The questionnaire was selected as a tool for data collection because it is easy to construct having the rules and principles of construction are easy to follow. Moreover, copies of the questionnaire can reach a considerable number of respondents either by mail or by personal distribution. Generally, responses to a questionnaire are objectified and standardized and these make tabulation easy. But more importantly, the respondent's replies will of their own free will because there will be no interviewer to influence them. This is one way to avoid biasness, particularly the interviewer's biasness.

3.3 DATA ANALYSIS

The data will be analysed from the various respondents on the surveyed sample to give information on the general trends. The two methods of analysis will be used, the frequency analysis and cross-tabulation analysis. The information from questionnaires will be summarized into figures or tables. In literature analysis a comparison criteria will be used to evaluate the previous and current work on the area of research.

3.4 CHAPTER SUMMARY

This chapter gives an account how the study will be carried out. The kinds of study qualitative and quantitative are elaborated in detail in the research design. The tool; interview is presented and reasons are given as to why this tool was selected among others. A description of sample population and the sampling technique is elaborated. The section ends with analysis which briefly explains how the sample data will be presented to get results.

4.0 ANALYSIS

4.1 GENERAL QUESTIONS AND RESULTS

This sub-section highlights the general questions posed to the members of the public and the police in order to assess their technological background.

There were two separate questionnaires; one for the members of the public and other one for the police. A total of 61 respondents participated in this study. 29 of them were police officers while the remaining were the members of public.

The genders of the respondents were not uniformly distributed with overall of 38 male and 23 female respondents. 6 respondents did not return the questionnaire after the survey.

The table below shows the distribution of the respondents.

Level		Gender		
	Respondents	Male	Female	No response
Police	29	20	9	4
Member of public	32	18	14	2

Table 2: Respondents distribution table
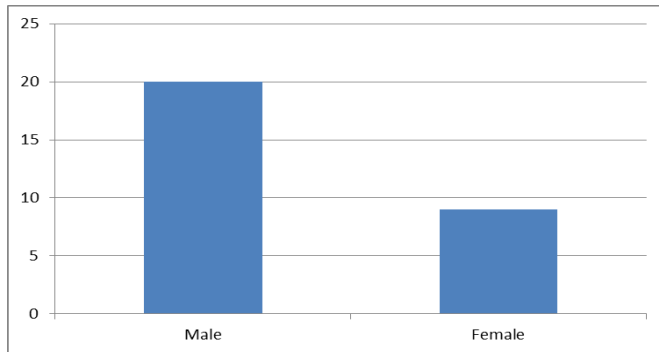
Figure 27 : Police respondents
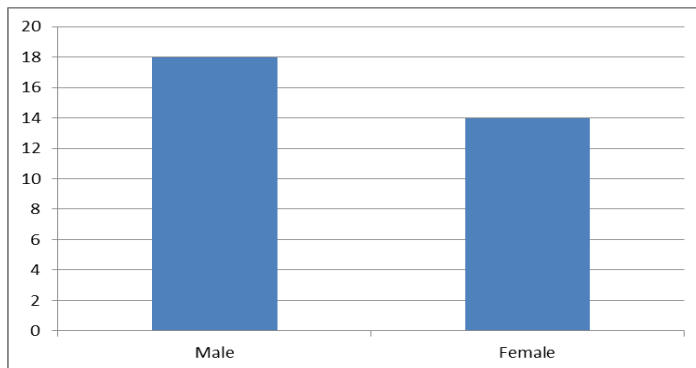
Figure 28 : Member of the public respondents

56

4.1.1   Members of the public

The below tables gives the questionnaire (Appendix B) results statistics from the respondents (member of the public):

Table 3: Do you own a mobile phone?

Yes	No
32	0

Table 4 : How long have you used mobile phone?

Never	Less than 1 year	2-4 Years	5 years and above
0	1	7	24

Table 5 : Do you use SMS daily?

Yes	No
30	2

Table 6 : How many times do you use SMS daily on average?

Never	Less than 1 hour	1-2 hours	5 hours and above
0	8	6	18

Table 7 : How many years have you been using SMS?

Never	Less than 1 year	2-4 years	5 years and above
0	1	9	22

Table 8 : Have you ever reported an incident or communicated to the police?

Yes	No
12	18

Table 9 : Which means do you use to communicate to the police?

Landline Telephone	Mobile call	SMS	E-mail	Face to face	Radio call	Other
1	9	1	1	17	0	2

Table 10 : Have you ever reported an incident or communicated to the police using your mobile device?

Yes	No
3	29

Table 11 : Have you ever sent an SMS to a police station?

Yes	No
1	31

Table 12 : Have you ever received an SMS from a police station?

Yes	No
0	32

The study shows that 100% of the respondents owned mobile phones (Table 3) and from table 4, 75% of the respondents having over 5 year experience of using mobile phone i.e.
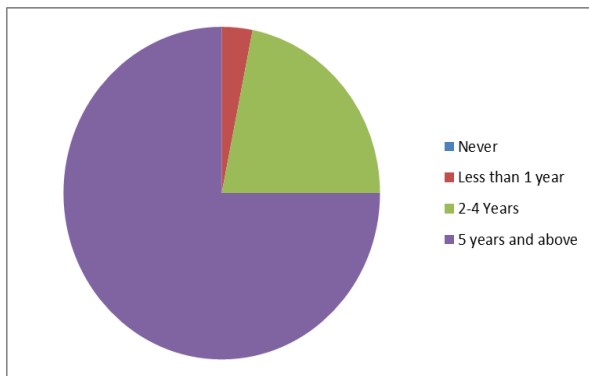
Figure 29 : Number of years using mobile phone

The study also shows that 94% of the respondents use SMS daily i.e.
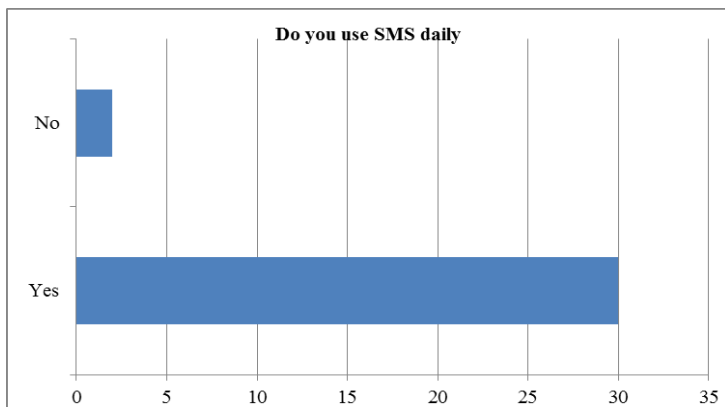
Figure 30 : Do you use SMS daily?

Narrowing down further as shown in table 7, the study also show that 69% of the respondents have been using SMS for 5 year and above followed closely by 28% who have the experience of the same for 2-4 years i.e.
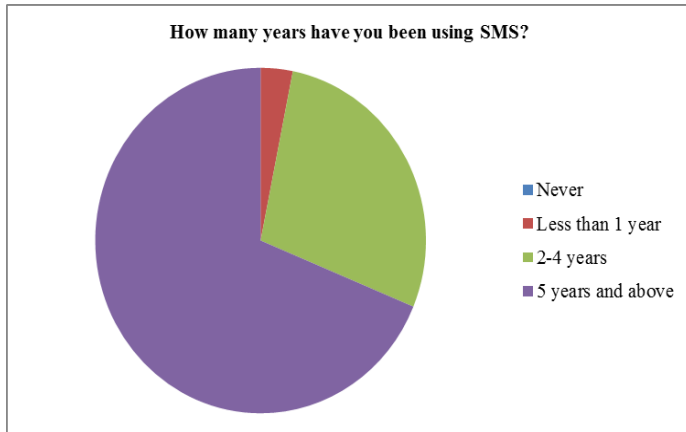
Figure 31 : How many years have you been using SMS?

Also from table 8 of the study a majority of the respondents have at least at one time reported or communicated to the police. The study further shows that a higher percentage of the respondents mostly prefer face to face means to communicate with the police as shown in table 9 and in figure 28. The next mode preferred by respondents is mobile calls.
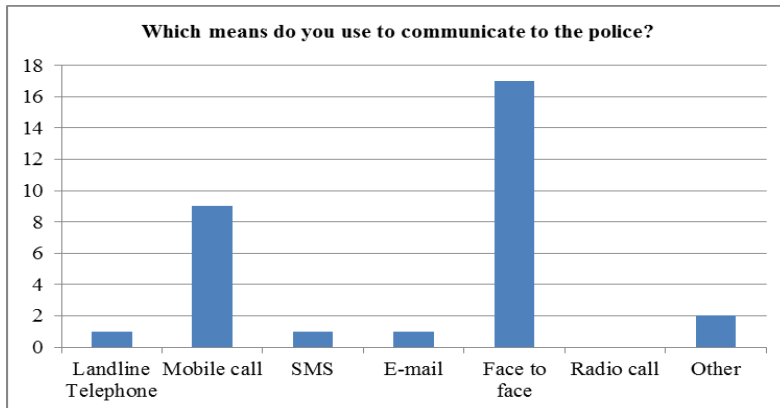
Figure 32 : Which means do you use to communicate to the police?

The study also shows (as seen in table 10) that 91% of the respondents have never reported or communicated to the police using mobile phone.
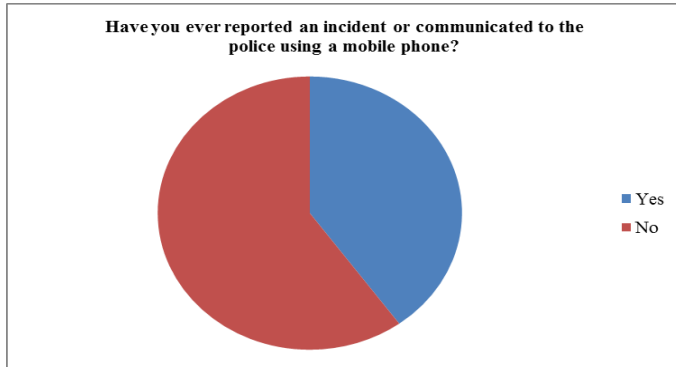
Figure 33 : Have you ever reported an incident or communicated to the police using a mobile phone?

In the study this is further shown that indeed even 97% of the respondents have never sent an SMS to a police station (table 11) as well as all respondents (table 12) have never received an SMS from a police station.
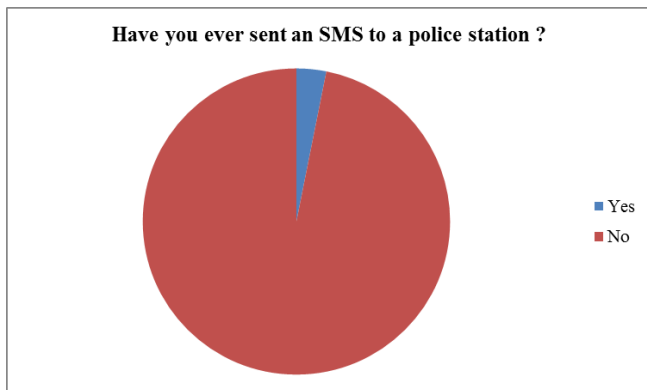
Figure 34 : Have you ever sent an SMS to a police station
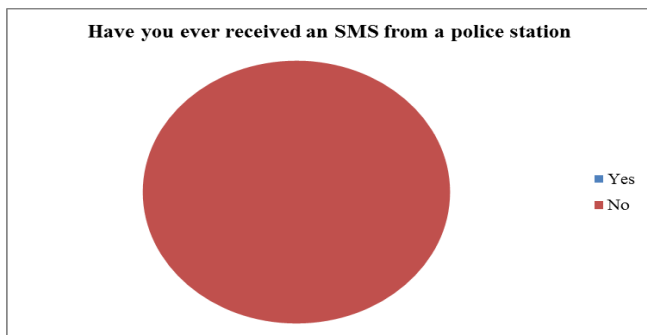
Figure 35 : Have you ever received an SMS from a police station?

4.1.1 __The police__

The below tables gives the questionnaire (Appendix B) results statistics from the respondents (the police):

Table 13: Do you own a mobile phone?

Yes	No
29	0

Table 14 : How long have you used mobile phone?

Never	Less than 1 year	2-4 Years	5 years and above
0	0	0	29

Table 15 : Do you use SMS daily?

Yes	No
25	4

Table 16 : How many times do you use SMS daily on average?

Never	Less than 1 hour	1-2 hours	5 hours and above
0	2	2	25

Table 17 : How many years have you been using SMS?

Never	Less than 1 year	2-4 years	5 years and above
0	0	0	29

Table 18 : Which means do you use mostly to communicate with other police officers in relation work matters?

Landline Telephone	Mobile call	SMS	E-mail	Face to face	Radio call	Other
0	22	5	0	16	15	1

Table 19 : Which means do you use mostly to communicate to the members of the public?

Landline Telephone	Mobile call	SMS	E-mail	Face to face	Radio call	Other
0	18	7	0	20	0	0

Table 20 : Have you ever reported an incident or communicated to the other police officers using your mobile device?

Yes	No
29	0

Table 21 : Have you ever sent an SMS to a police station?

Yes	No
21	8

Table 22 : Have you ever received an SMS from a police station?

Yes	No
9	20

From the police response, the study shows that all the respondents own mobile phones (Table 13) with over 5 years' experience of using them (Table 14).

The study also shows (Table 15) that 86% of the respondents use SMS daily with all the respondents having over 5 years' experience of SMS usage (Table 17) i.e.
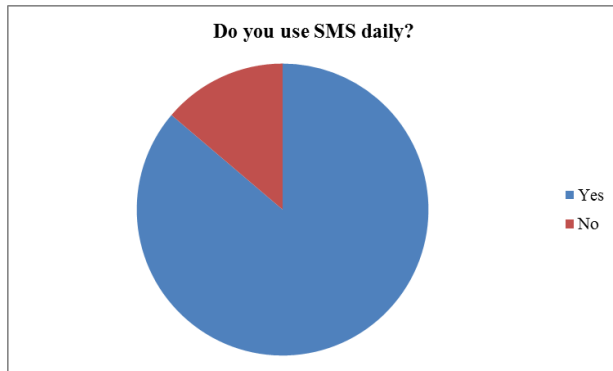
Figure 36 : Do you use SMS daily?

From table 18, the study also shows that most respondents use mobile calls, followed by face to face and radio call in that order to communicate to each other on work related matters:
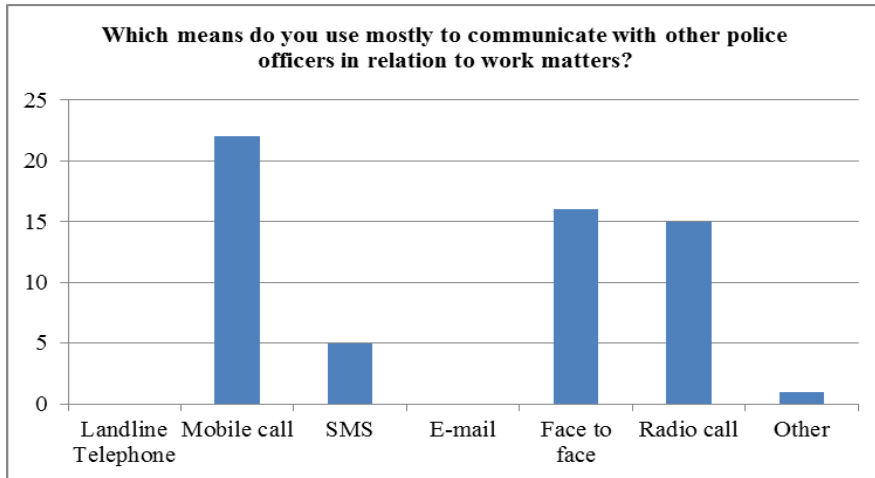
Figure 37: which means to you use mostly to communicate to other police officers in relation to work matters?

From Table 19, the study shows that respondents mostly use face to face communication to communication with the members of the public. The respondents also prefer using mobile phone calls as the next means of communication with the member of the public:
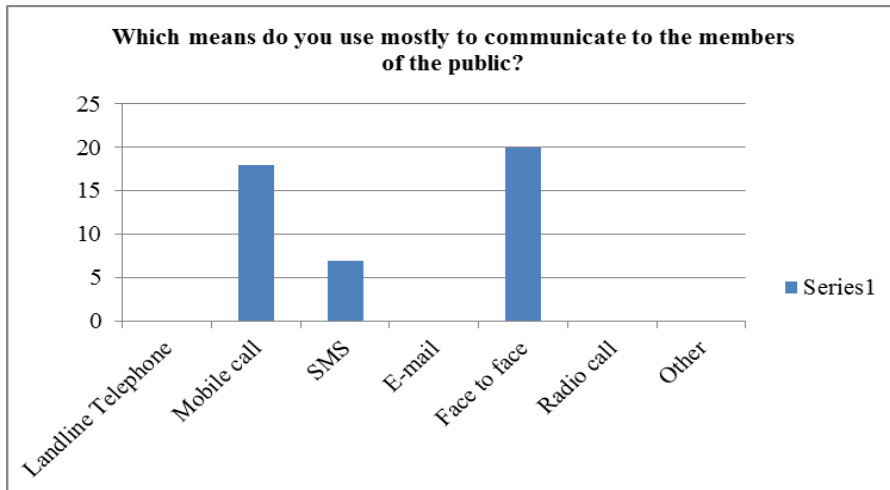

Figure 38 : Which means do you use mostly to communicate to the members of the public?

Table 20 shows that all the respondents in the study have use their mobile phones at one time to communicate to other officers. This is further shown by the statistics of the respondents sending and receiving of SMS (Tables 21 and Table 22) to and from a police station. 72% of the respondents have at one time sent an SMS to a police station. On the other hand 70% of the respondents have never received an SMS from a police station.
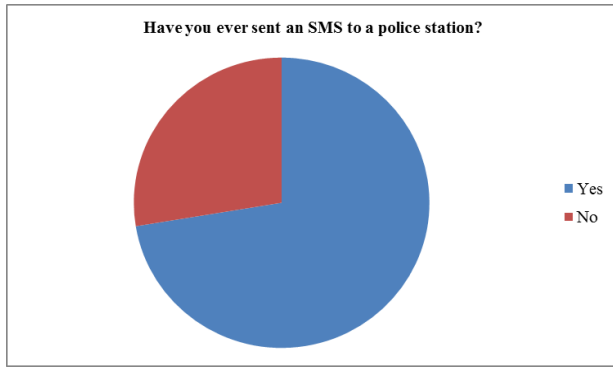
Figure 39 : Have you ever sent an SMS to a police station?
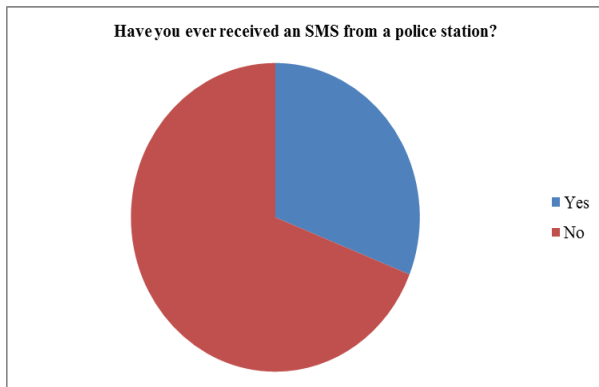
Figure 40 : Have you ever received an SMS from a police station?

4.2 PROTOTYPE REQUIREMENTS

From the analysis, an SMS gateway (system) that needs to be in place should have the following capabilities:

- Web bases system interface for centralized access.

- System authentication mechanisms for all the users.

- Permit sending an SMS to a single mobile phone e.g. the communication controller can route a specific SMS to an individual police officer.

- Permit sending of an SMS broadcast to a group of police officers for action on a certain issue of concern.

- Possess inboxes where specific alerts are received from the members of the public or from police boses seniors in matters of alert. E.g. inbox for patrol officers, traffic officers etc

- A single incoming security alert SMS should be routed from a mobile phone to various police groups / departments for action.

64

4.3 CHAPTER SUMMARY

This chapter highlights in details the analysis work done. Survey responses on the technological background including communication means used by both members of the public and the police are highlighted. Lastly in the chapter a list of the prototype requirements are listed.

5.0 DESIGN AND IMPLEMENTATION

5.1 SMS GATEWAY ARCHITECTURE

This project used one GSM phone (acting as a modem) attached to a laptop (serving as an SMS gateway server).
The GSM phone was connected to the laptop via a USB cable.
Fedora 20 Operating System was installed on the laptop followed by Kannel and Playsms configurations.

Kannel is an open source SMS gateway for GSM networks.

Open source (http://www.opensource.org) is a way to formalize the principle of openness by placing the source code of a product under a Open Source compliant software license. The BSD license was chosen over other Open Source licenses by the merit of placing the lease amount of limitations on what a third party is able to do with the source code.   In practice this means that Kannel is going to be a fully-features SMS implementation and compatible with the maximum number of bearers with special emphasis on SMSC compatibility. The Kannel project was founded by Wapit Ltd in June, 1999.

When SMS services are used, the client (mobile terminal) sends an SMS messages to certain number, usually a very short specialized number, which points to specific SMS center responsible for that number (plus possibly many others). This SMS center then sends the message onward to specified receiver in intra or internet, using an SMS centres specific protocol.

An SMS gateway is used to handle connections with SMS centers and to relay them onwards in an unified form. Kannel's biggest feature is to abstract each SMSC protocol to a well-known HTTP protocol, simplifying services deployment.

Kannel is being developed on Linux systems and is very to easy to export to other Unix-like systems.

Kannel installed required the following software environment:

- C compiler and libraries for ANSI C

- The Gnome XML library (known as gnome-xml and libxml)

- GNU make

- An implementation of POSIX threads (pthread.h)

Hardware requirements are fluffier, some informal benchmarking have shown that with a reasonably fast PC architecture (e.e. 400MHz Pentium II with 128MB RAM), SMS performance bottleneck is always on the SMSC side, even though for example with multiple connections summing a pipeline with 400 msg/sec.

Kannel consists of three programs called boxes:

The bearer box: is the interface towards the phones, it accepts SMS & WAP messages from the phones and sends them to the other boxes.

The SMS box: handles SMS gateway functionality.

**The WAP box**: handles WAP gateway functionality.

5.2 SMS GATEWAY WEB PORTAL

For the web-based portal for this project, playsms (playsms.org) was used. This is the Graphical User Interface of the SMS gateway through which the Administrator carries out administrative tasks of the gateway including sending and receiving SMS. Other users can also send / receive SMS through this portal.

Playsms is a flexible Open Source system that can be made to interface various services such as an SMS gateway, personal messaging systems, corporate and group communication tools.

Playsms as a web portal was installed in the same hardware (laptop) where Kannel was installed and configured.

As a result the portal was accessed through address: http://localhost/nairobi-police-sms

An administrator and other system users log into the system by supplying the correct username and password. This presents them with the below home page:
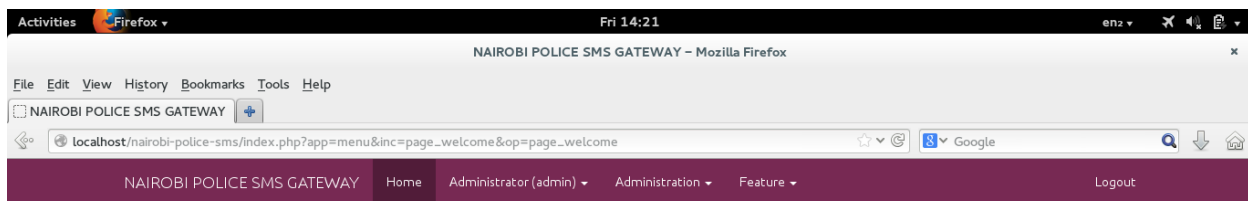
5.2.1   SOFTWARE REQUIREMENTS FOR PLAYSMS

Playsms required the following software as a prerequisite for its installation and configuration:

- – Webserver (apache)

- – MySQL database server 4.x.x or latest stable release

- – PHP 4.4 or latest stable release

- – PHP PEAR DB

- – Lynx, a console web browser.

5.2.2   USER ROLES

There are 2 roles in the SMS gateway portal:

- Administrator
- Normal User

Users are created in the system based on the above two roles.

Administrator privileges in the Portal

An administrator manages the overall functionality of the gateway.

An administrator has privilege to:

- Manage users:
  - Add users
  - Modify users
  - Delete users
- Monitor all incoming and outgoing SMS (all users's inboxes).
- Manage the SMS gateway:
  - Add settings
  - Modify settings
  - Delete settings
- View SMS gateway logs

Normal User privileges in the Portal

Normal users have no administrative privileges in the SMS gateway.

They can only:

- Manage their phone book entries:
  - Add, modify or delete groups
  - Add, modify or delete contacts
- Send SMS to a group or single mobile number
- Check their incoming SMS
- Check their outgoing SMS

- Set their preferences:

  - Change their login passwords

  - Update personal information

- Use other features of the gateway:

  - Autoreply

  - Board

  - Command

  - Custom

  - Poll

  - Quiz

  - Subscribe

  - sync

5.3 FUNCTIONAL MODULES IN SMS GATEWAY

The SMS gateway has several modules i.e.:

- Login module

- Home module

- Search module

- Contacts module

- Administration module

- Users module

- Logout module

i. <u>LOGIN MODULE</u>

This module is used for authenticating users by ensuring that the username and password supplied matches what is in the database.

The figure below shows the login screen:

ii. HOME MODULE

This is the main interface; it shows all links for all features available for a specific user depending on the privileges.

The figure below shows the home module:
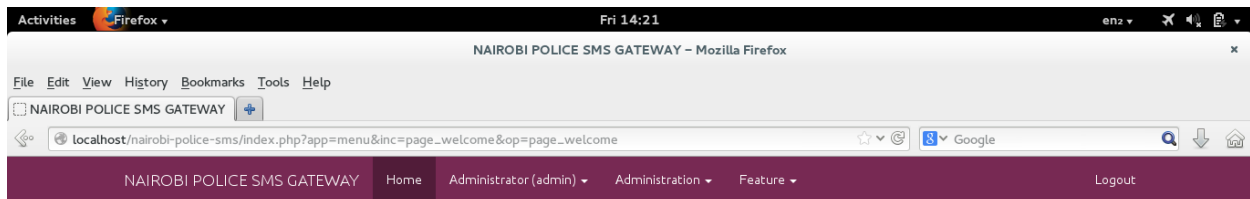
iii.   <u>SEARCH MODULE</u>

The search module is used across in various sections. Users can perform search in:

- Phonebook using either:

  - Name

  - Mobile

  - Email

  - Group code

- Incoming SMS using either:

  - Name

  - Mobile

  - Email

  - Group code

- Outgoing SMS using either:

  - Time

  - From

  - Keyword

  - Content

  - Feature

An example of searching in the phonebook is shown below:

Input search of name "Duncan"

Result of the search:

iv.   CONTACTS MODULE

In this module:

- Groups can be added and assigned a group code and name as show below:
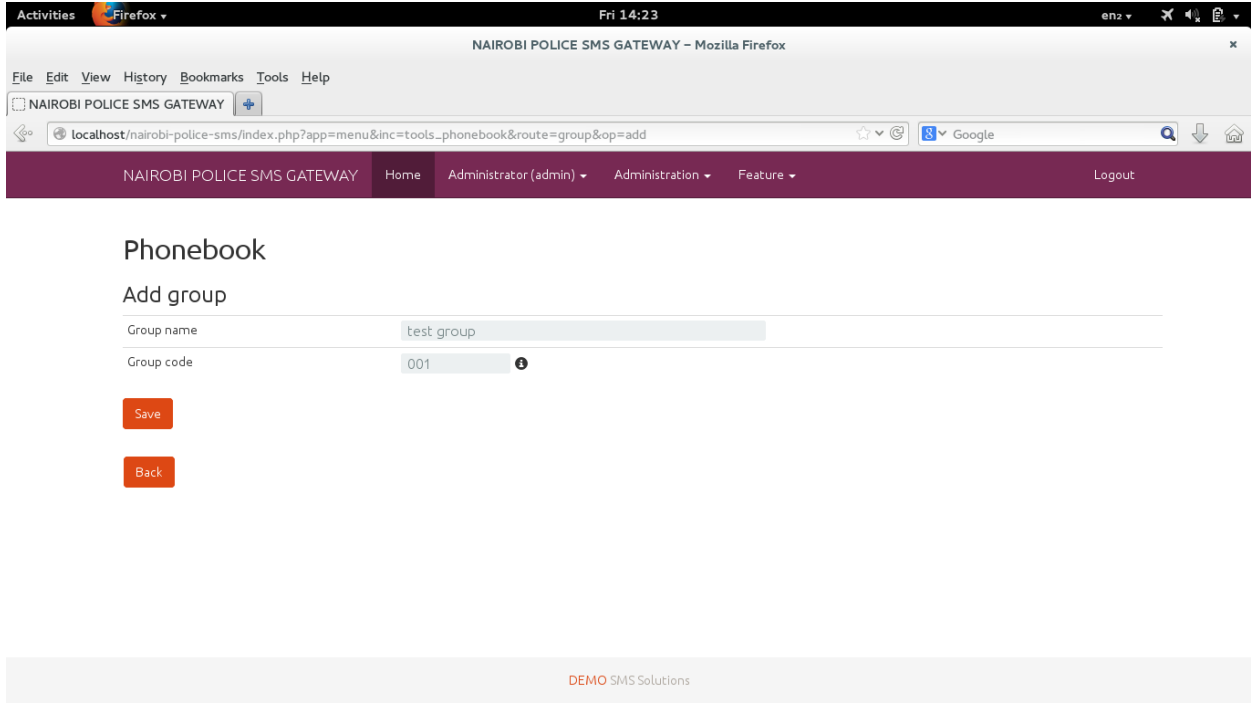
- Contacts can be to a group added as shown:
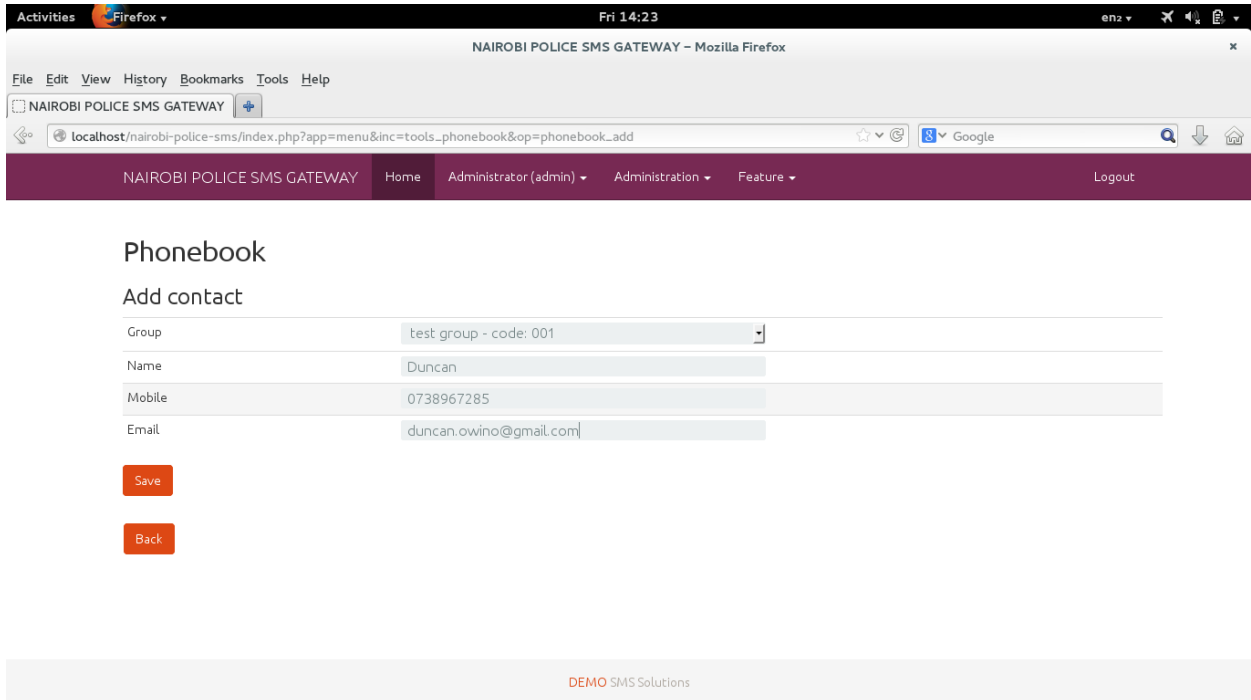
v.   ADMINISTRATION MODULE

This is an important module in the SMS gateway. This module consists of the following sub-modules:

- All inboxes module

- All incoming SMS module

- All outgoing SMS module

- All reports module

- Main configuration module

- Manage user module

- Manage SMS rate module

- Manage Gateway module

- Manage plugin module

- View SMS queue module

- View log module

All inboxes module

This module shows the contents of the inboxes of all the users in the system. These details can be searched, modified or deleted.
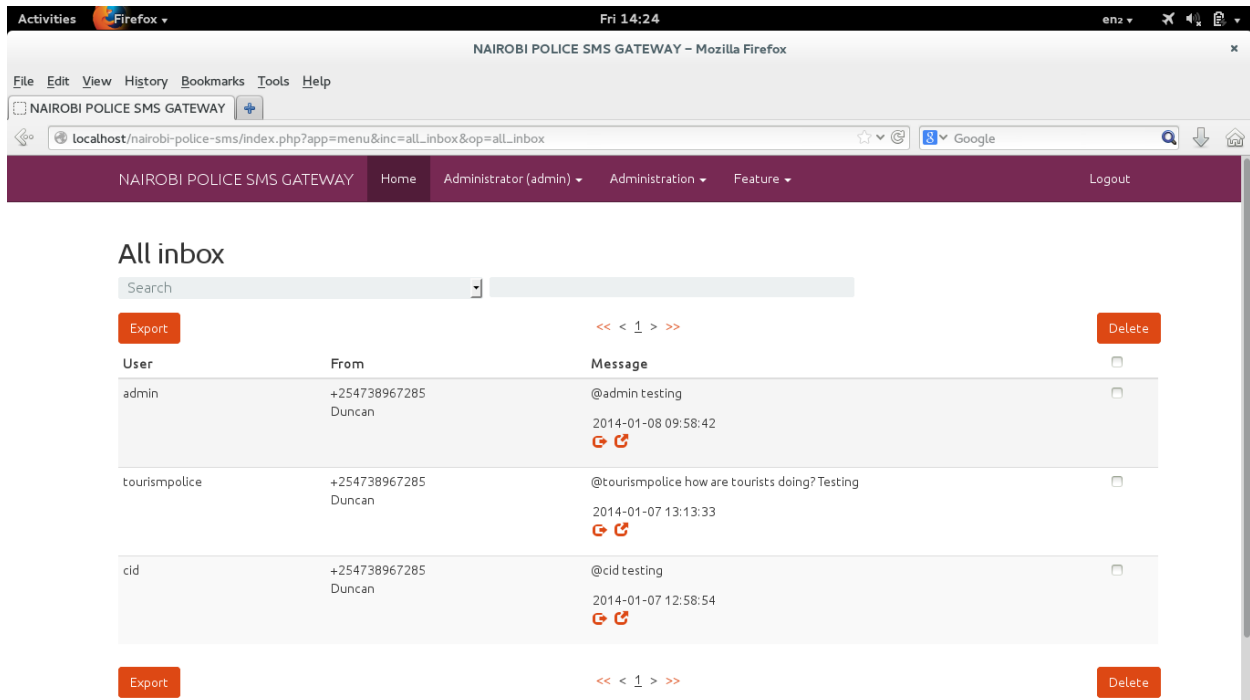
All incoming SMS module

This shows all incoming SMS for all users. The details of source of the SMS, keyword (if any) and message contents are shown. These details can be searched, modified or deleted.

All outgoing SMS module

This shows all outgoing SMS for all users. The details of the user, destination of the SMS and message contents are shown.

All reports module

This shows states on pending, sent, delivered or failed and billing information of SMS for each users in the system.

Main configuration module

In this module the global settings that affect all uses in the system are applied, modified or deleted here. For example timezone, default credit for each user etc.

Manage user module

This module is used to add, modify or delete a user from the system.

Manage Gateway module

This module offers the provision to add, modify and activate a specific gateway. In our case as seen below, Kannel is the only gateway that has been activated.

vi.   USERS MODULE

This module permits the user to have the following capabilities:

vii. LOGOUT MODULE

This module is used to logout users from the system.

5.4 *THE STORAGE STRUCTURE OF THE SMS GATEWAY*

Playsms uses Mariadb (a fork db of MySQL) which is an open source database software. The database created for this project in MySQL is "playsms". It holds a total of 58 tables as shown below:

```
MariaDB [playsms]> show tables;
+----------------------------------+
| Tables_in_playsms                |
+----------------------------------+
| playsms_featureAutoreply
| playsms_featureAutoreply_scenario
| playsms_featureAutosend
| playsms_featureAutosend_time
| playsms_featureBoard
| playsms_featureBoard_log
| playsms_featureCommand
| playsms_featureCustom
| playsms_featureInboxgroup
| playsms_featureInboxgroup_catchall
| playsms_featureInboxgroup_log_in
| playsms_featureInboxgroup_log_out
| playsms_featureInboxgroup_members
| playsms_featurePoll
| playsms_featurePoll_choice
| playsms_featurePoll_log
| playsms_featureQuiz
| playsms_featureQuiz_log
| playsms_featureSmssysnc
| playsms_featureSubscribe
| playsms_featureSubscribe_member
| playsms_featureSubscribe_msg
| playsms_featureSurvey
| playsms_featureSurvey_log
| playsms_featureSurvey_members
| playsms_featureSurvey_questions
| playsms_gatewayClickatell_apidata
| playsms_gatewayClickatell_config
| playsms_gatewayGnokii_config
| playsms_gatewayInfobip_apidata
| playsms_gatewayInfobip_config
| playsms_gatewayKannel_config
| playsms_gatewayMsgtoolbox
| playsms_gatewayMsgtoolbox_config
| playsms_gatewayNexmo
| playsms_gatewayNexmo_config
| playsms_gatewaySmstools_dlr
| playsms_gatewayTemplate_config
| playsms_gatewayTwilio
| playsms_gatewayTwilio_config
| playsms_gatewayUplink
```

```
| playsms_gatewayUplink_config
| playsms_tblBilling
| playsms_tblConfig_main
| playsms_tblDLR
| playsms_tblRecvSMS
| playsms_tblRegistry
| playsms_tblSMSIncoming
| playsms_tblSMSOutgoing
| playsms_tblSMSOutgoing_queue
| playsms_tblSMSOutgoing_queue_dst
| playsms_tblUser
| playsms_tblUserInbox
| playsms_tblUser_country
| playsms_toolsMsgtemplate
| playsms_toolsPhonebook
| playsms_toolsPhonebook_group
| playsms_toolsSendfromfile
| playsms_toolsSimplerate
+----------------------------------+
```

The key tables are:

```
+----------------------------------+
| playsms_featureInboxgroup
| playsms_featureInboxgroup_catchall
| playsms_featureInboxgroup_log_in
| playsms_featureInboxgroup_log_out
| playsms_featureInboxgroup_members
| playsms_gatewayKannel_config
| playsms_tblBilling
| playsms_tblConfig_main
| playsms_tblDLR
| playsms_tblRecvSMS
| playsms_tblSMSIncoming
| playsms_tblSMSOutgoing
| playsms_tblSMSOutgoing_queue
| playsms_tblSMSOutgoing_queue_dst
| playsms_tblUser
| playsms_tblUserInbox
| playsms_toolsPhonebook
| playsms_toolsPhonebook_group
```

a. playsms_featureInboxgroup

This table stores inbox for specific groups.

The table structure is shown in the figure below below:

Field	Type	Null	Key	Default	Extra
c_timestamp	bigint(20)	NO		0	
id	int(11)	NO	PRI	NULL	auto_increment
uid	int(11)	NO		0	
in_receiver	varchar(20)	NO			
keywords	varchar(100)	NO			
description	varchar(250)	NO			
creation_datetime	varchar(20)	NO		0000-00-00 00:00:00	
exclusive	int(11)	NO		0	
deleted	int(11)	NO		0	
status	int(11)	NO		0	

b. playsms_featureInboxgroup_catchall

This table stores all the inbox for all groups as seen by the administrator.

The table structure is shown below:

Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	auto_increment
rid	int(11)	NO		0	
uid	int(11)	NO		0	

c. playsms_featureInboxgroup_log_in

The table structure is shown below:

Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	auto_increment
rid	int(11)	NO		0	
sms_datetime	varchar(20)	NO		0000-00-00 00:00:00	
sms_sender	varchar(20)	NO			
keyword	varchar(100)	NO			
message	text	NO		NULL	
sms_receiver	varchar(20)	NO			

d. playsms_featureInboxgroup_log_out

The table structure is shown below:

Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	auto_increment
log_in_id	int(11)	NO		0	
smslog_id	int(11)	NO		0	
catchall	int(11)	NO		0	
uid	int(11)	NO		0	

e. playsms_featureInboxgroup_members

The table structure is shown below:

Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	auto_increment
rid	int(11)	NO		0	
uid	int(11)	NO		0	

f. playsms_gatewayKannel_config

This table stores Kannel configuration information.

The table structure is shown below:

Field	Type	Null	Key	Default	Extra
c_timestamp	bigint(20)	NO		0	
cfg_name	varchar(20)	NO		kannel	
cfg_incoming_path	varchar(250)	YES		NULL	
cfg_username	varchar(100)	YES		NULL	
cfg_password	varchar(100)	YES		NULL	
cfg_global_sender	varchar(20)	YES		NULL	
cfg_bearerbox_host	varchar(250)	YES		NULL	
cfg_sendsms_host	varchar(250)	YES		NULL	
cfg_sendsms_port	varchar(10)	YES		NULL	
cfg_playsms_web	varchar(250)	YES		NULL	
cfg_dlr	int(11)	NO		31	
cfg_additional_param	varchar(250)	YES		NULL	
cfg_datetime_timezone	varchar(30)	NO		700	
cfg_admin_url	varchar(250)	YES		NULL	

cfg_admin_password	varchar(50)	YES		NULL	
cfg_admin_port	int(11)	NO		0	

g. playsms_tblBilling

This table stores billing information.

The table structure is shown below:

Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	auto_increment
c_timestamp	bigint(20)	NO		0	
post_datetime	varchar(20)	NO		0000-00-00 00:00:00	
smslog_id	int(11)	NO		0	
rate	decimal(10,2)	NO		0	
credit	decimal(10,2)	NO		0	
count	int(11)	NO		0	
charge	decimal(10,2)	NO		0	
status	int(11)	NO		0	

h. playsms_tblConfig_main

This table stores main configuration information.

The table structure is shown below:

Field	Type	Null	Key	Default	Extra
c_timestamp	bigint(20)	NO		0	
cfg_web_title	varchar(250)	YES		NULL	
cfg_email_service	varchar(250)	YES		NULL	
cfg_email_footer	varchar(250)	YES		NULL	
cfg_gateway_module	varchar(20)	YES		NULL	
cfg_gateway_number	varchar(100)	YES		NULL	
cfg_themes_module	varchar(100)	YES		NULL	
cfg_default_rate	decimal(10,2)	NO		0	
cfg_language_module	varchar(10)	YES		en_US	
cfg_datetime_timezone	varchar(30)	NO		700	
cfg_sms_max_count	int(11)	NO		3	
cfg_default_credit	decimal(10,2)	NO		0	
cfg_enable_register	int(11)	NO		0	

cfg_enable_forgot	int(11)	NO		1	
cfg_allow_custom_sender	int(11)	NO		0	
cfg_allow_custom_footer	int(11)	NO		0	
cfg_main_website_name	varchar(250)	NO			
cfg_main_website_url	varchar(250)	NO			

i. playsms_tblDLR

This table stores SMS delivery status information.

The table structure is shown below:

Field	Type	Null	Key	Default	Extra
c_timestamp	bigint(20)	NO		0	
id	int(11)	NO	PRI	NULL	auto_increment
flag_processed	int(11)	NO		0	
smslog_id	int(11)	NO		0	
p_status	int(11)	NO		0	
uid	int(11)	NO		0	

j. playsms_tblRecvSMS

This table stores received SMS.

The table structure is shown below

Field	Type	Null	Key	Default	Extra
c_timestamp	bigint(20)	NO		0	
id	int(11)	NO	PRI	NULL	auto_increment
flag_processed	int(11)	NO		0	
sms_datetime	varchar(20)	NO		0000-00-00 00:00:00	
sms_sender	varchar(20)	NO			
message	text	NO		NULL	
sms_receiver	varchar(20)	NO			

k. playsms_tblSMSIncoming

This table stores incoming SMS.

The table structure is shown below:

Field	Type	Null	Key	Default	Extra
c_timestamp	bigint(20)	NO		0	
in_id	int(11)	NO	PRI	NULL	auto_increment
flag_deleted	int(11)	NO		0	
in_uid	int(11)	NO		0	
in_feature	varchar(250)	NO			
in_gateway	varchar(100)	NO			
in_sender	varchar(100)	NO			
in_receiver	varchar(20)	NO			
in_keyword	varchar(100)	NO			
in_message	text	NO		NULL	
in_datetime	varchar(20)	NO		0000-00-00 00:00:00	
in_status	int(11)	NO		0	

l. playsms_tblSMSOutgoing

This table stores outgoing SMS.

The table structure is shown below:

Field	Type	Null	Key	Default	Extra
c_timestamp	bigint(20)	NO		0	
id	int(11)	NO	PRI	NULL	auto_increment
smslog_id	int(11)	YES	UNI	NULL	
flag_deleted	int(11)	NO		0	
uid	int(11)	NO		0	
p_gateway	varchar(100)	NO			
p_src	varchar(100)	NO			
p_dst	varchar(100)	NO			
p_footer	varchar(30)	NO			
p_msg	text	NO		NULL	
p_datetime	varchar(20)	NO		0000-00-00 00:00:00	
p_update	varchar(20)	NO		0000-00-00 00:00:00	
p_status	int(11)	NO		0	
p_gpid	int(11)	NO		0	
p_credit	decimal(10,2)	NO		0	
p_sms_type	varchar(100)	NO			

Field	Type	Null	Key	Default	Extra
unicode	int(11)	NO		0	
queue_code	varchar(40)	NO			

m. playsms_tblSMSOutgoing_queue

This table stores SMSes in queue.

The table structure is shown below:

Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	auto_increment
queue_code	varchar(40)	NO	UNI		
datetime_entry	varchar(20)	NO		000-00-00 00:00:00	
datetime_scheduled	varchar(20)	NO		000-00-00 00:00:00	
datetime_update	varchar(20)	NO		000-00-00 00:00:00	
flag	int(11)	NO		0	
sms_count	int(11)	NO		0	
uid	int(11)	NO		0	
gpid	int(11)	NO		0	
sender_id	varchar(100)	NO			
footer	varchar(30)	NO			
message	text	NO		NULL	
sms_type	varchar(100)	NO			
unicode	int(11)	NO		0	

n. playsms_tblSMSOutgoing_queue_dst

This table stores SMSes in queue and their destinations.

The table structure is shown below:

Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	auto_increment
queue_id	int(11)	NO		0	
smslog_id	int(11)	NO		0	
flag	int(11)	NO		0	
dst	varchar(50)	NO			

o. playsms_tblUser

This table stores all the information of all users in the system.

The table structure is shown below:

Field	Type	Null	Key	Default	Extra
c_timestamp	bigint(20)	NO		0	
uid	int(11)	NO	PRI	NULL	auto_increment
status	int(11)	NO		0	
ticket	varchar(100)	NO			
username	varchar(100)	NO			
password	varchar(32)	NO			
token	varchar(32)	NO			
enable_webservices	int(11)	NO		0	
webservices_ip	varchar(100)	NO			
name	varchar(100)	NO			
mobile	varchar(16)	NO			
email	varchar(250)	NO			
sender	varchar(16)	NO			
footer	varchar(30)	NO			
address	varchar(250)	NO			
city	varchar(100)	NO			
state	varchar(100)	NO			
country	int(11)	NO		0	
zipcode	varchar(10)	NO			
credit	decimal(10,2)	NO		0	
datetime_timezone	varchar(30)	NO		700	
language_module	varchar(10)	NO		en_US	
fwd_to_mobile	int(11)	NO		0	
fwd_to_email	int(11)	NO		1	
fwd_to_inbox	int(11)	NO		1	
replace_zero	varchar(5)	NO			
plus_sign_remove	int(11)	NO		1	
plus_sign_add	int(11)	NO		0	
send_as_unicode	int(11)	NO		0	
local_length	int(11)	NO		9	
register_datetime	varchar(20)	NO		0000-00-00 00:00:00	
lastupdate_datetime	varchar(20)	NO		0000-00-00 00:00:00	

p. playsms_tblUserInbox

This table stores all the SMS inbox information for a user.

The table structure is shown below:

Field	Type	Null	Key	Default	Extra
c_timestamp	bigint(20)	NO		0	
in_id	int(11)	NO	PRI	NULL	auto_increment
in_sender	varchar(20)	NO			
in_receiver	varchar(20)	NO			
in_uid	int(11)	NO		0	
in_msg	varchar(200)	NO			
in_datetime	varchar(20)	NO		0000-00-00 00:00:00	
in_hidden	int(11)	NO		0	

q. playsms_toolsPhonebook

This table stores all the contacts for a user.

The table structure is shown below:

Field	Type	Null	Key	Default	Extra
c_timestamp	bigint(20)	NO		0	
id	int(11)	NO	PRI	NULL	auto_increment
gpid	int(11)	NO		0	
uid	int(11)	NO		0	
mobile	varchar(100)	NO			
name	varchar(250)	NO			
email	varchar(250)	NO			

r. playsms_toolsPhonebook_group

This table stores all the groups data as added by a user.

The table structure is shown below

Field	Type	Null	Key	Default	Extra
c_timestamp	bigint(20)	NO		0	
id	int(11)	NO	PRI	NULL	auto_increment
uid	int(11)	NO		0	
name	varchar(100)	NO			
code	varchar(20)	NO			

5.5 CHAPTER SUMMARY

The chapter begins by describing the SMS gateway architecture and how it was configured. It also describes the various roles in the SMS gateway and the modules in the system. Finally the database structure of the SMS gateway is provided in the chapter.

6.0 RESULTS AND DISCUSSION

6.1 SURVEY DESIGN

In this section, an explanation of the survey design of this study is given.

The survey was carried out in various estates of Nairobi and police stations/posts across some police divisions in Nairobi.

First the SMS gateway (system) was installed and configured. All the participants in the study (police and members of the public) participated voluntarily. Those who agreed were supposed to have any GSM mobile phone that can be able to send and receive SMS. They shared the mobile phone numbers voluntarily in order to test the functionality of the SMS gateway.

They were required to send an SMS to a specific inbox as well as receive from the same source.

For the police officers, they were required to access the SMS gateway portal http://localhost/nairobi-police-sms by supplying correct username and password. They were then required to add at least a phone number in the gateway phonebook after creating groups. This was followed by sending/receiving of SMS using the gateway.

The study participants had questionnaires administered to them after a prototype demonstration i.e. they were required to fill on their usage of the gateway and return their feedback for analysis.

The questionnaires were collected and put into 2 bands; the member of public and the police groups. The participants who agreed to be interviewed were given a letter of transmittal for their consent to participate in the interview.

6.2 PROTOTYPE EVALUATION (FINDINGS OF SURVEY)

This section provides the outcome of the survey conducted in Nairobi in January 2014 on the SMS gateway usage for security enhancement.

The instrument used in this study was questionnaire as shown in the appendix section B and C. Members of the public and the police were involved in this study.

6.2.1   Questionnaire findings

There were two separate questionnaires; one for the members of the public and other one for the police. The administered questionnaires were divided into 3 sections A, B and C. Section A was used to gather personal details; section B gathered technological background details while part C gathered SMS gateway (system) usage details. A likert type scale was used in part C ranging from "Strongly agree" to "Neutral".

A total of 61 respondents participated in this study. 29 of them were police officers while the remaining were the members of public.

The genders of the respondents were not uniformly distributed with overall of 38 male and 23 female respondents. 6 respondents did not return the questionnaire after the survey.

The table below shows the distribution of the respondents.

Level		Gender		
	Respondents	Male	Female	No response
Police	29	20	9	4
Member of public	32	18	14	2

Table 23: Respondents distribution table
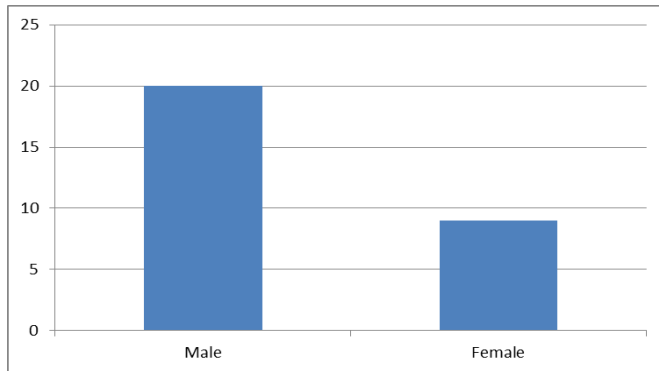
Figure 41 : Police respondents
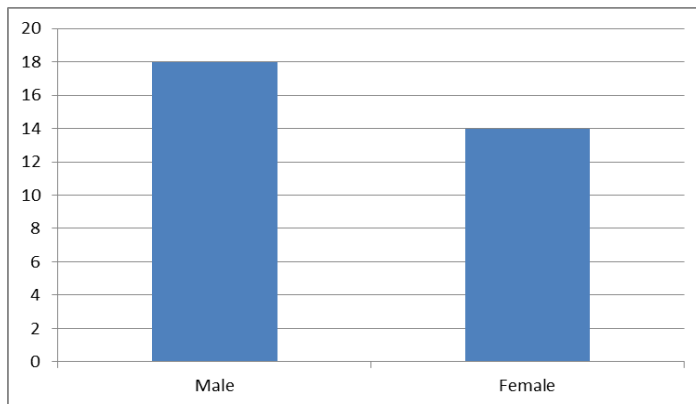
Figure 42 : Member of the public respondents

3.4.1 Results SMS Gateway (System) Usage results (Members of the public)

In the last part of the questionnaire (section C), a total of 14 statements were used to assess various aspects of the SMS gateway (System). A likert scale was used.

Statement 1: *It is easy to send SMS from the SMS system (gateway)*

All the members of the public in the study replied to this statement. Most of them strongly agree (21), others agree (10) while only 1 was neutral to this statement.
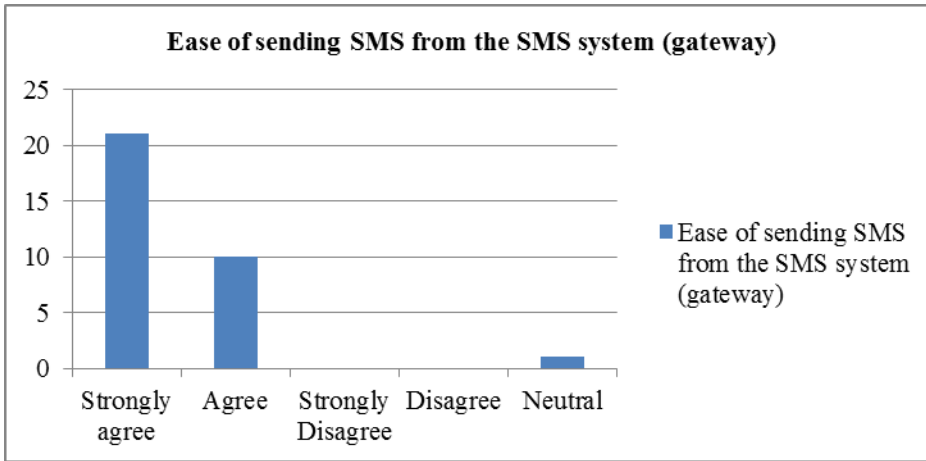
Figure 43 - Easy to send SMS from the SMS system (gateway)

Statement 2: *It is easy to receive SMS from the SMS (gateway) using my mobile phone*

All the members of the public in the study replied to this statement. Most of them strongly agree (23) while others agree (9) to this statement.
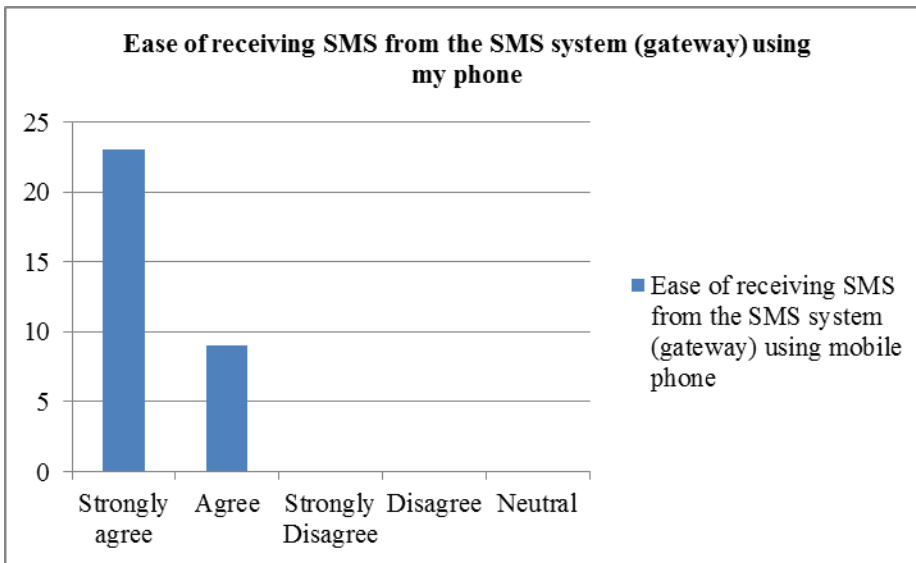
Figure 44 - Easy to receive SMS from the SMS (gateway) using my mobile phone

Statement 3: *I can get SMS from the SMS system anywhere and anytime I want using the SMS system*

All the members of the public in the study replied to this statement. Most of them strongly agree (22), others agree (7), while the rest remain neutral (3) to this statement.
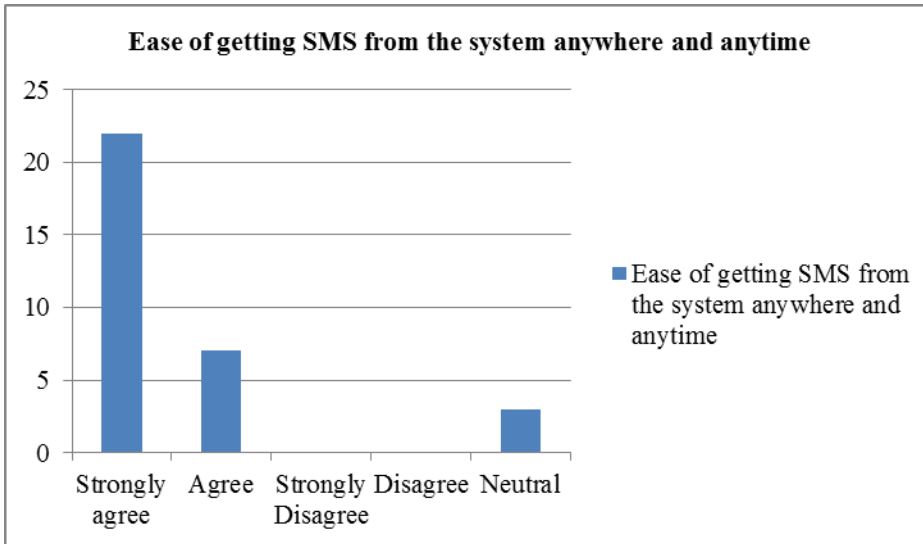
Figure 45 - I can get SMS from the SMS system anywhere and anytime I want using the SMS system

Statement 4: *It is more convenient to send important alerts to the police using the SMS system*

All the members of the public in the study replied to this statement. Most of them strongly agree (23), others agree (7), while the rest remain neutral (2) to this statement.
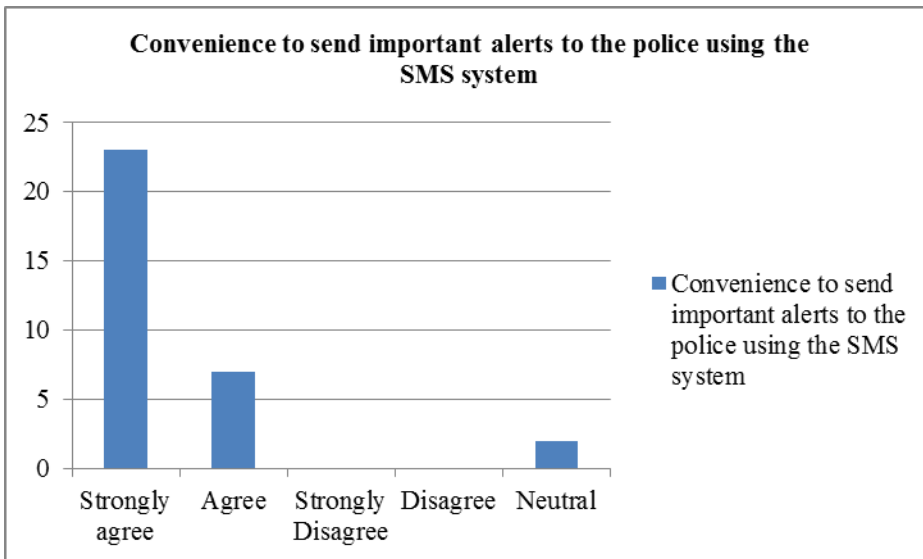
Figure 46 - It is more convenient to send important alerts to the police using the SMS system

Statement 5: *It is more convenient to receive important alerts from the police using the SMS system*

All the members of the public in the study replied to this statement. Most of them strongly agree (23), others agree (5), while the rest remain neutral (4) to this statement
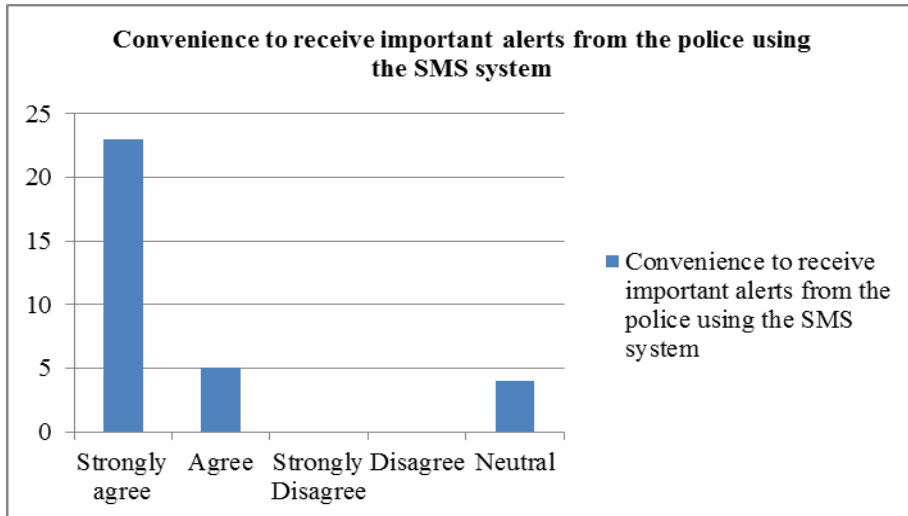
Figure 47 - It is more convenient to receive important alerts from the police using the SMS system

Statement 6: *It is possible to provide alert information to police using the SMS system*

All the members of the public in the study replied to this statement. Most of them strongly agree (23) while the rest agree (9) to this statement

Figure 48 - It is possible to provide alert information to police using the SMS system

Statement 7: *It is possible to receive alert information from Police using the SMS system*

All the members of the public in the study replied to this statement. Most of them strongly agree (21), others agree (9) while the rest remain neutral (2) to this statement
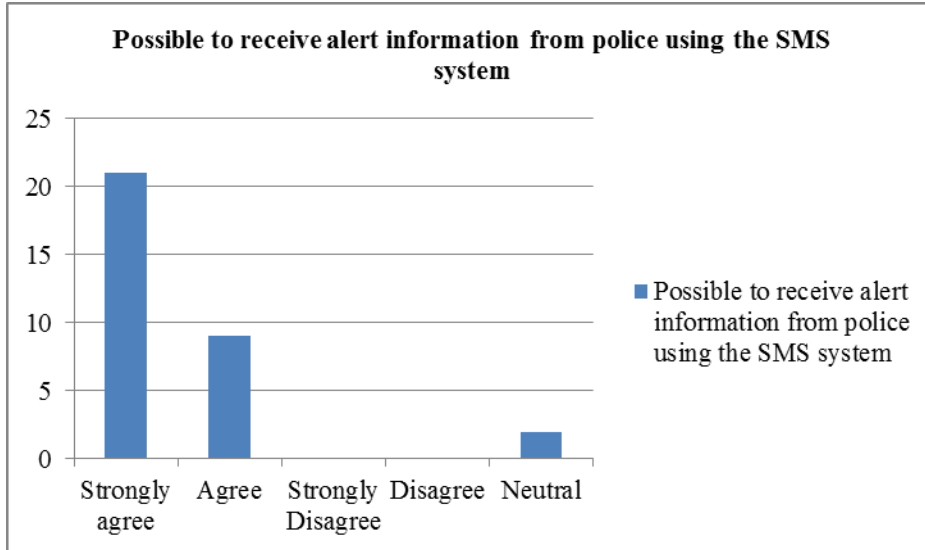
Figure 49 - It is possible to receive alert information from Police using the SMS system

Statement 8: *It is possible to increase security measures by using SMS to report to the police*

All the members of the public in the study replied to this statement. Most of them strongly agree (17), others agree (14) while the only one remain neutral (1) to this statement.
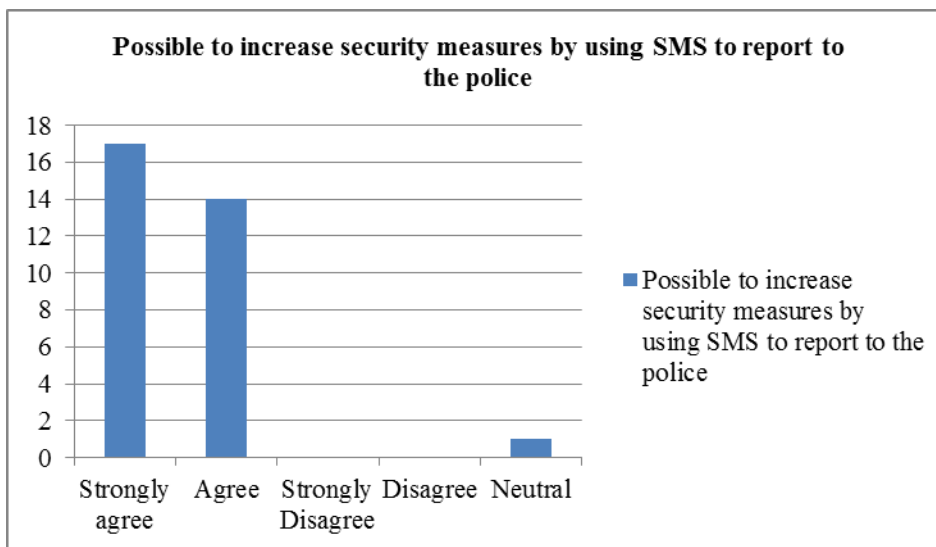

Figure 50 - It is possible to increase security measures by using SMS to report to the police

Statement 9: *Sending SMS using the system did not take long*

All the members of the public in the study replied to this statement. Most of them strongly agree (23), others agree (8) while the only one remain neutral (1) to this statement.
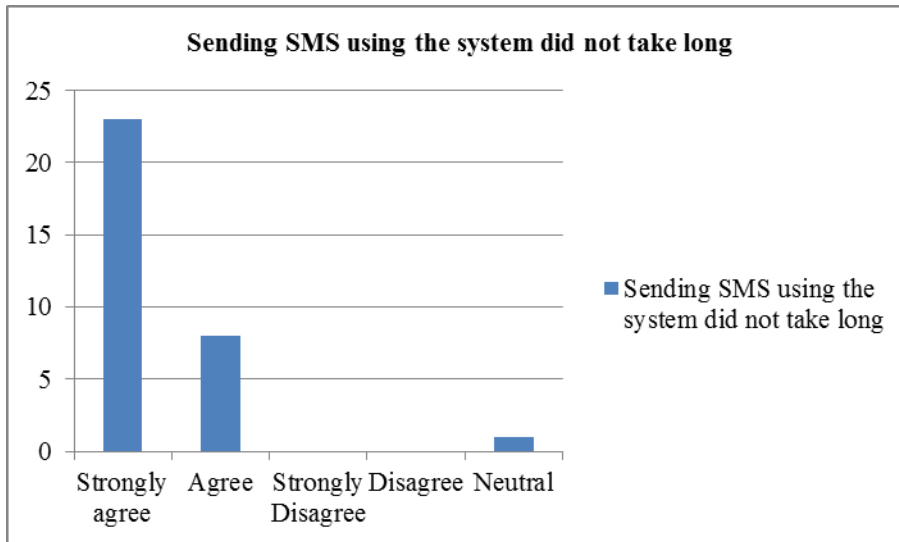
Figure 51 - Sending SMS using the system did not take long

Statement 10: *Receiving an SMS using the system did not take long*

All the members of the public in the study replied to this statement. Most of them strongly agree (23), others agree (8) while the only one remain neutral (1) to this statement.
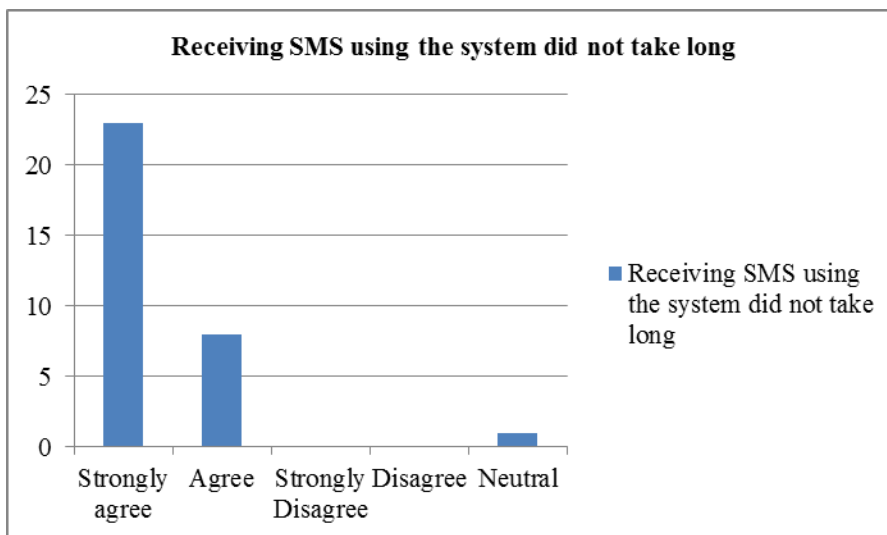
Figure 52 - Receiving an SMS using the system did not take long

Statement 11: *The menu items were well labeled and easy to follow*

All the members of the public in the study replied to this statement. Most of them strongly agree (19) while the rest agree (13) to this statement.
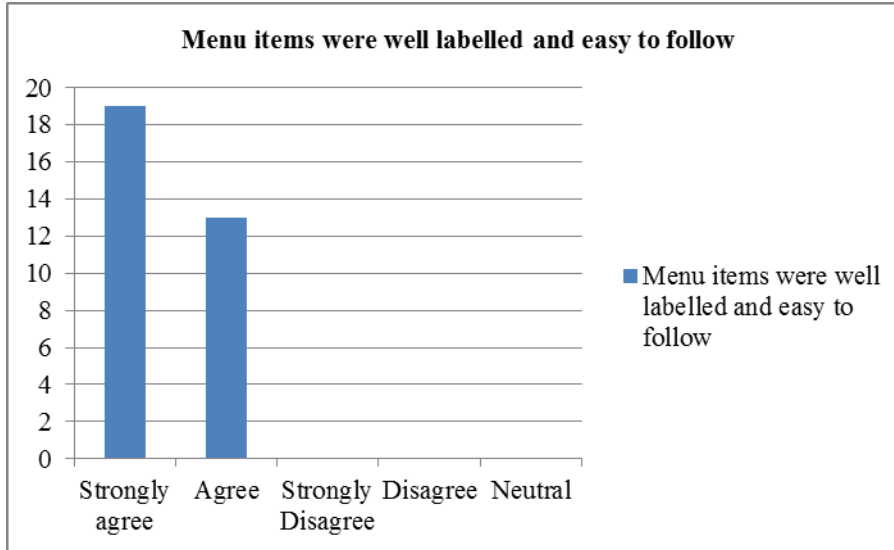

Figure 53 - The menu items were well labeled and easy to follow

Statement 12: *Navigation links allow quick access to various functionalities*

All the members of the public in the study replied to this statement. Most of them strongly agree (15) and Agree (15), only one disagree (1) and the last one remains neutral (1) to this statement.
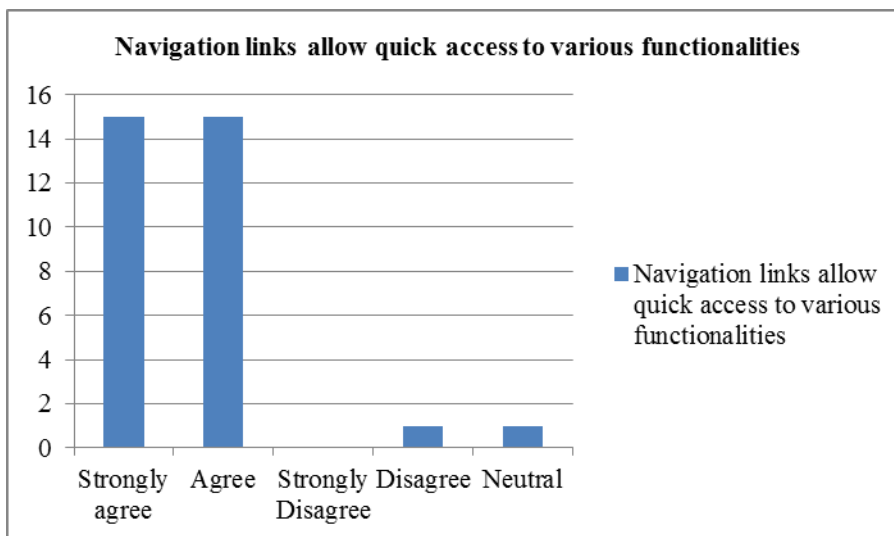
Figure 54 - Navigation links allow quick access to various functionalities

Statement 13: *Consistent page structure in all web interfaces*

All the members of the public in the study replied to this statement. Most of them strongly agree (16), some agree (12) while the rest remain neutral (4) to this statement
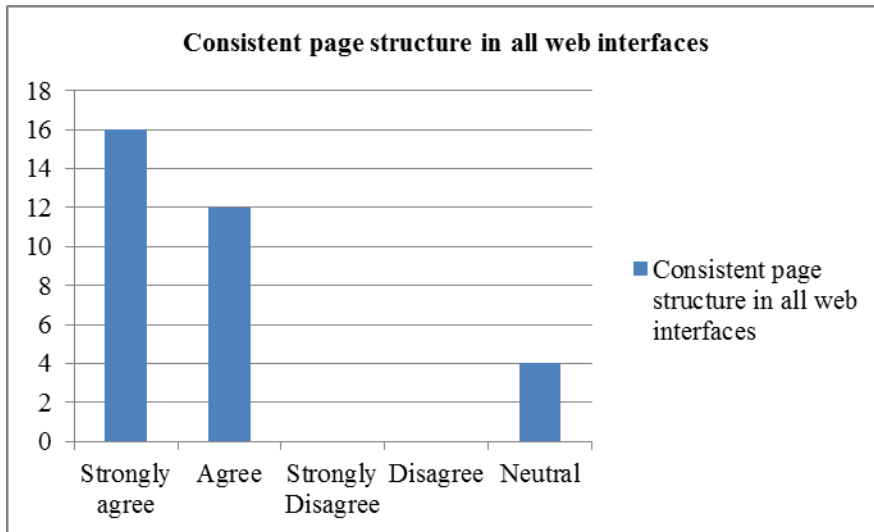

Figure 55 - Consistent page structure in all web interfaces

Statement 14: *There were adequate access control mechanisms to ensure only registered users can access the system.*

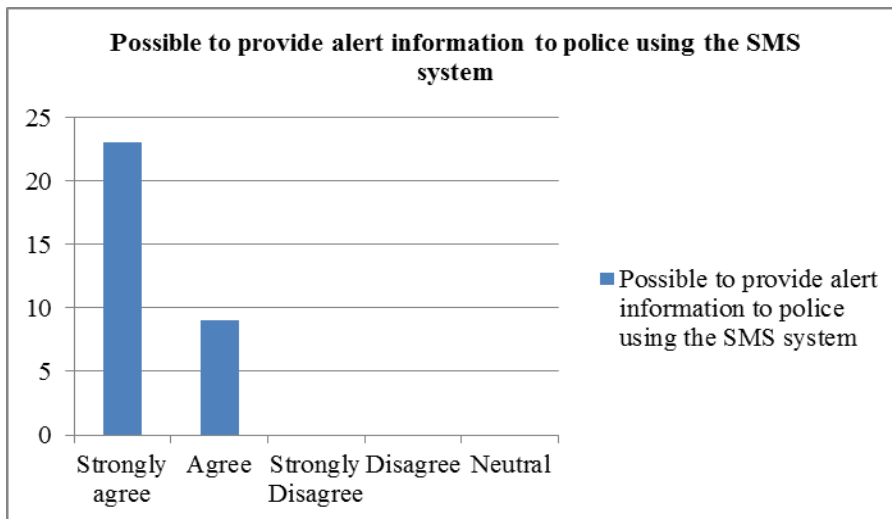All the members of the public in the study replied to this statement. Most of them strongly agree (16), some agree (12) while the rest remain neutral (4) to this statement
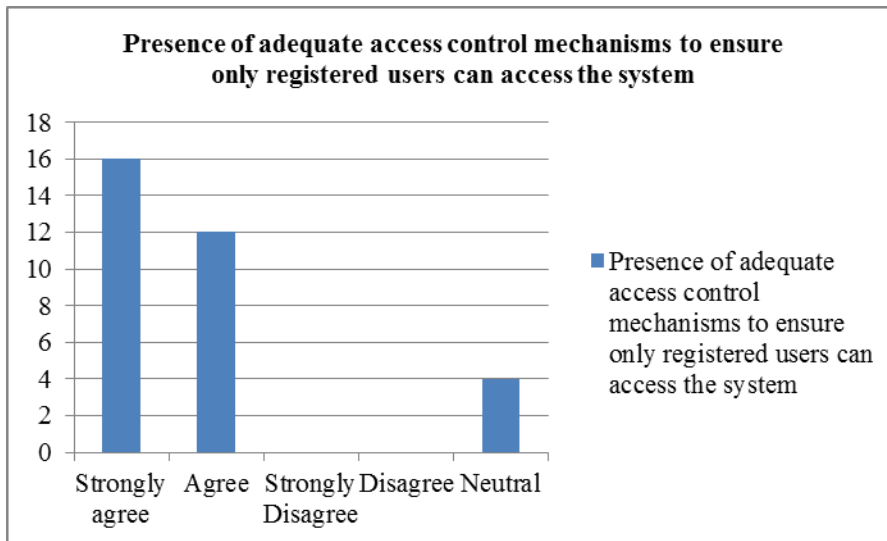

Figure 56 - Adequate access control mechanisms to ensure only registered users can access the system.

98

3.4.2 Results SMS Gateway (System) Usage results (The Police)

In the last part of the questionnaire (section C), a total of 14 statements were used to assess various aspects of the SMS gateway (System). A likert scale was used.

Statement 1: *It is easy to send SMS from the SMS system (gateway)*

All the police officers in the study replied to this statement. Most of them strongly agree (27) while the rest agree (2) to this statement.
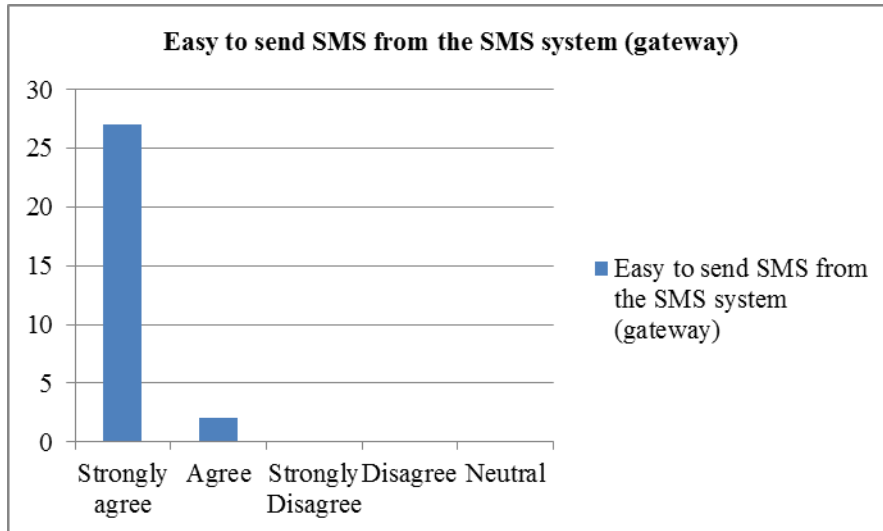
Figure 57 - Easy to send SMS from the SMS system (gateway)

Statement 2: *It is easy to receive SMS from the SMS (gateway) using my mobile phone*

All the police officers in the study replied to this statement. Most of them strongly agree (25), some agree (3) while only one disagrees (1) with this statement.
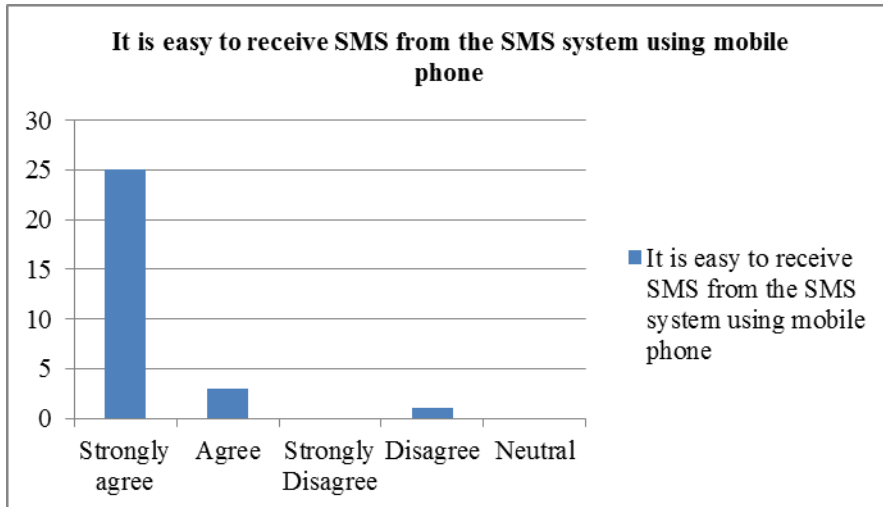
Figure 58 - It is easy to receive SMS from the SMS (gateway) using my mobile phone

Statement 3: *I can get SMS from the SMS system anywhere and anytime I want using the SMS system*

All the police officers in the study replied to this statement. Most of them strongly agree (23), some agree (5) while only one remains neutral (1) to this statement.
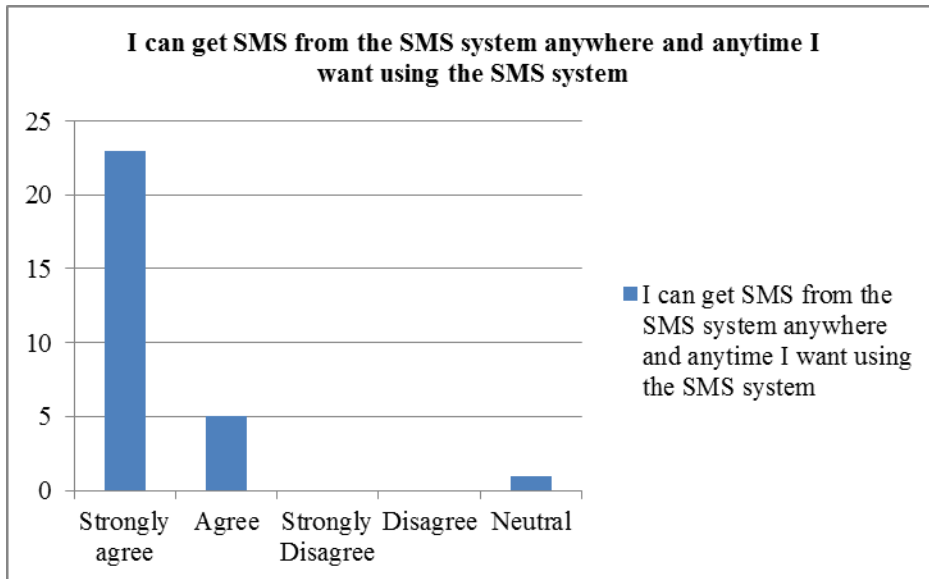

Figure 59 - I can get SMS from the SMS system anywhere and anytime I want using the SMS system

Statement 4: *It is more convenient to send important alerts to other police officers using the SMS system*

All the police officers in the study replied to this statement. Most of them strongly agree (23) while the rest agree (6) to this statement.

Convenient to send important alerts to other police officers using the SMS system
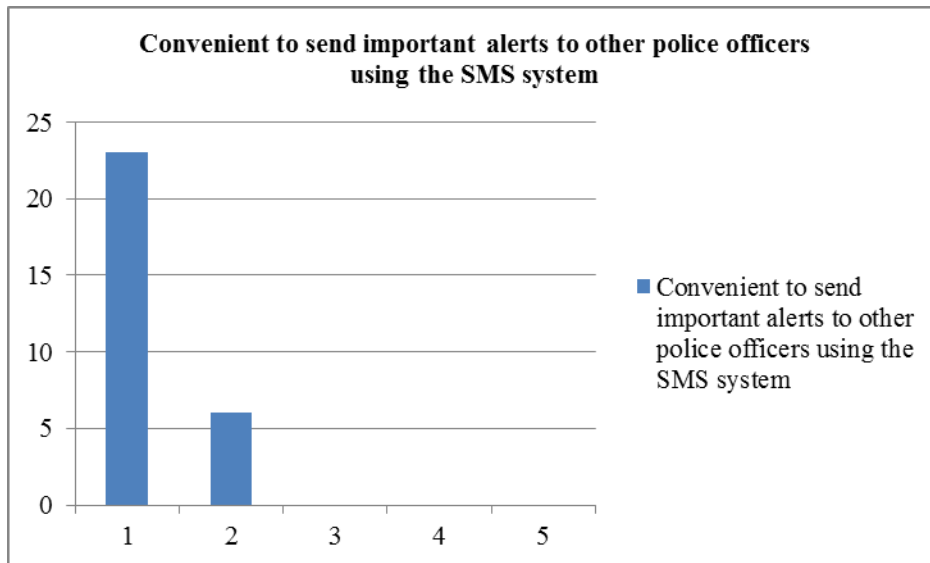
Figure 60 - It is more convenient to send important alerts to other police officers using the SMS system

Statement 5: *It is more convenient to receive important alerts from other police officers using the SMS system*

All the police officers in the study replied to this statement. Most of them strongly agree (23), some agree (4) while the rest strongly disagree (2) to this statement.


Convenient to receive important alerts from other police officers using the SMS system
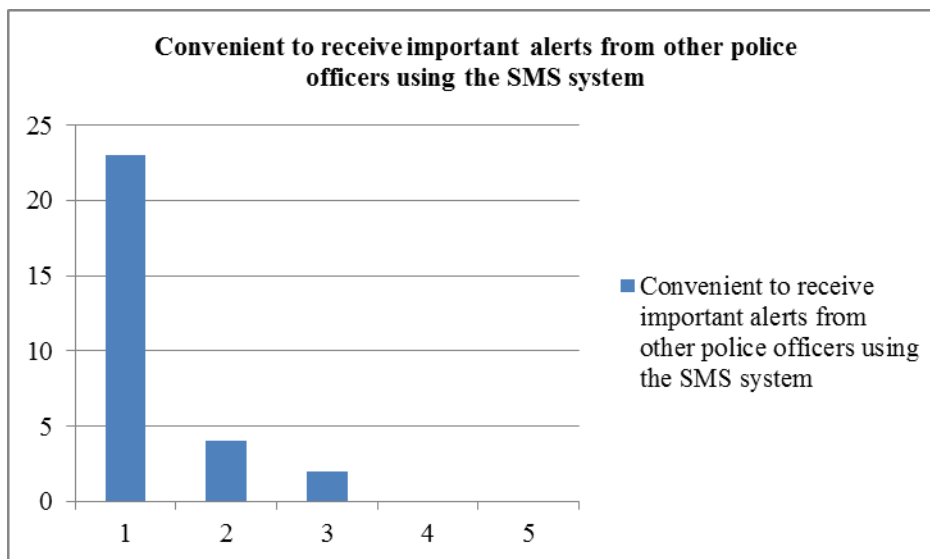
Figure 61 - It is more convenient to receive important alerts from other police officers using the SMS system

Statement 6: *It is possible to provide alert information to police using the SMS system*

All the police officers in the study replied to this statement. Most of them strongly agree (24), some agree (4) while only one disagrees (1) with this statement.
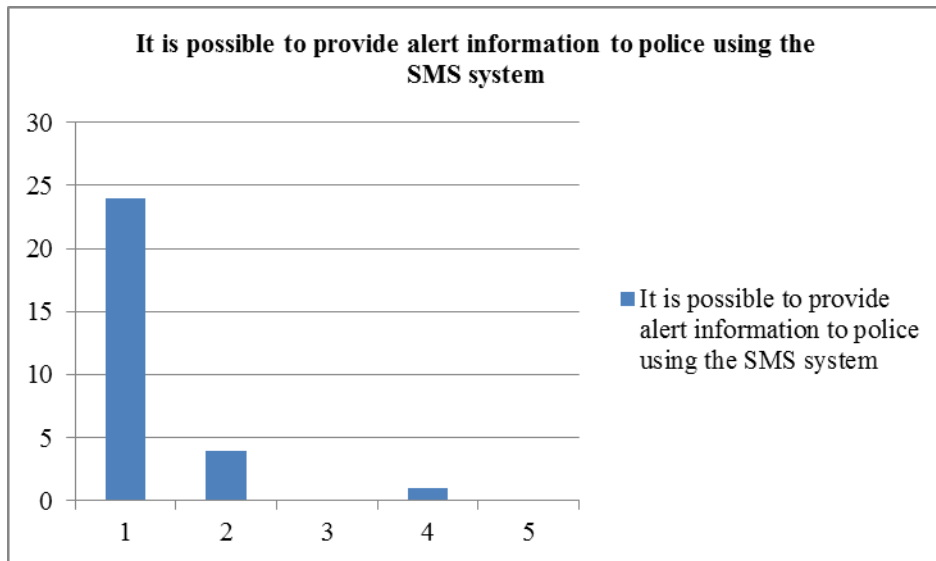
Figure 62 - It is possible to provide alert information to police using the SMS system

Statement 7: *It is possible to receive alert information from Police using the SMS system*

All the police officers in the study replied to this statement. Most of them strongly agree (22), some agree (6) while only one strongly disagrees (1) with this statement.
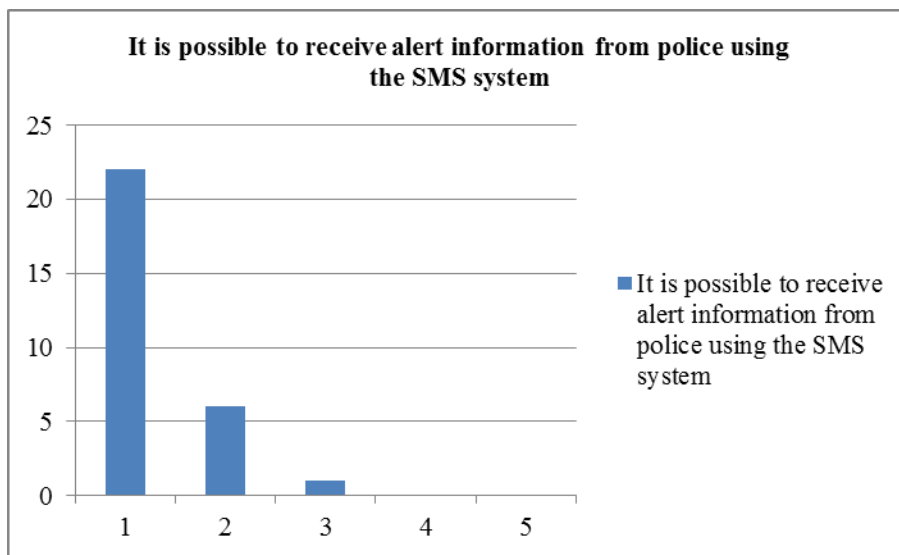
Figure 63 - It is possible to receive alert information from Police using the SMS system

Statement 8: *It is possible to increase security measures by using SMS to report to the police*

All the police officers in the study replied to this statement. Most of them strongly agree (24), some agree (3), one strongly disagrees (1) to this statement. There is also one that remains neutral (1) to this statement.
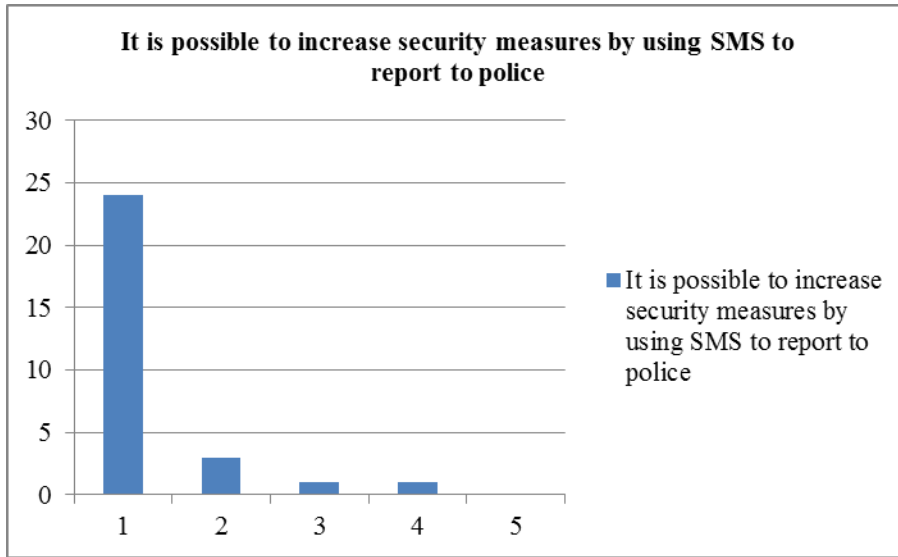
Figure 64 - It is possible to increase security measures by using SMS to report to the police

Statement 9: *Sending SMS using the system did not take long*

All the police officers in the study replied to this statement. Most of them strongly agree (24) while the rest agree (5) with this statement.
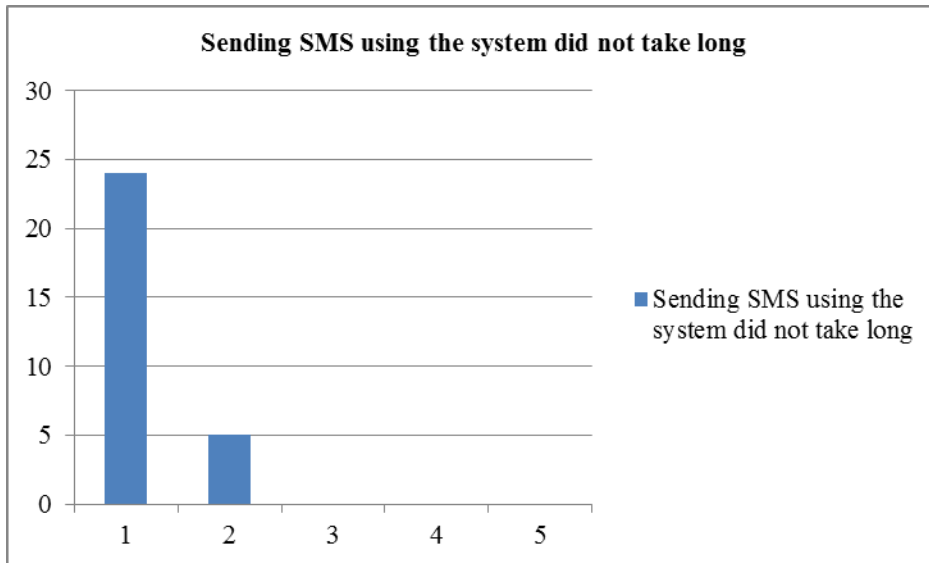
Figure 65 - Sending SMS using the system did not take long

Statement 10: *Receiving an SMS using the system did not take long*

All the police officers in the study replied to this statement. Most of them strongly agree (22) while the rest agree (7) with this statement.

103
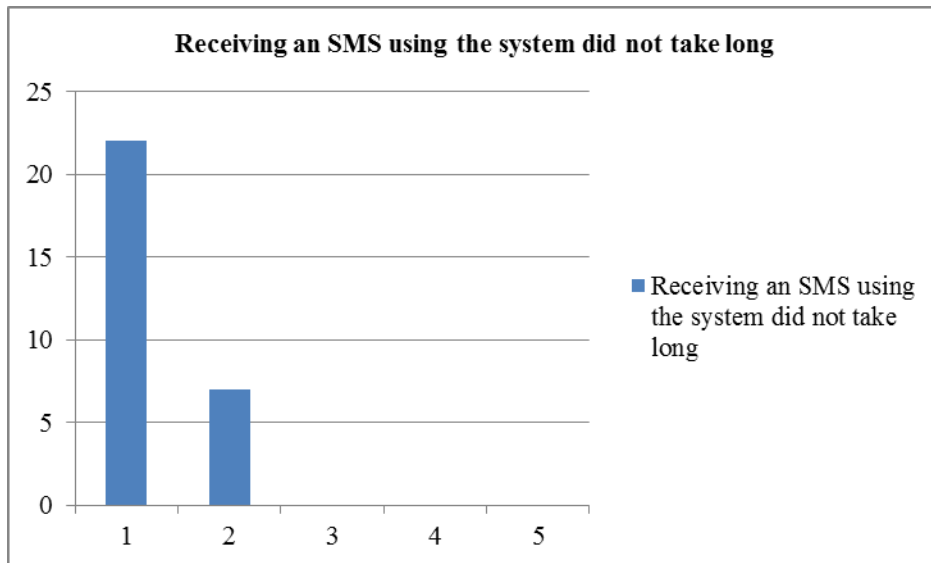
Figure 66 - Receiving an SMS using the system did not take long

Statement 11: *The menu items were well labelled and easy to follow*

All the police officers in the study replied to this statement. Most of them strongly agree (24), three agree (3) while another one strongly disagrees (1) with this statement. One respondent remained neutral (1) to this statement.
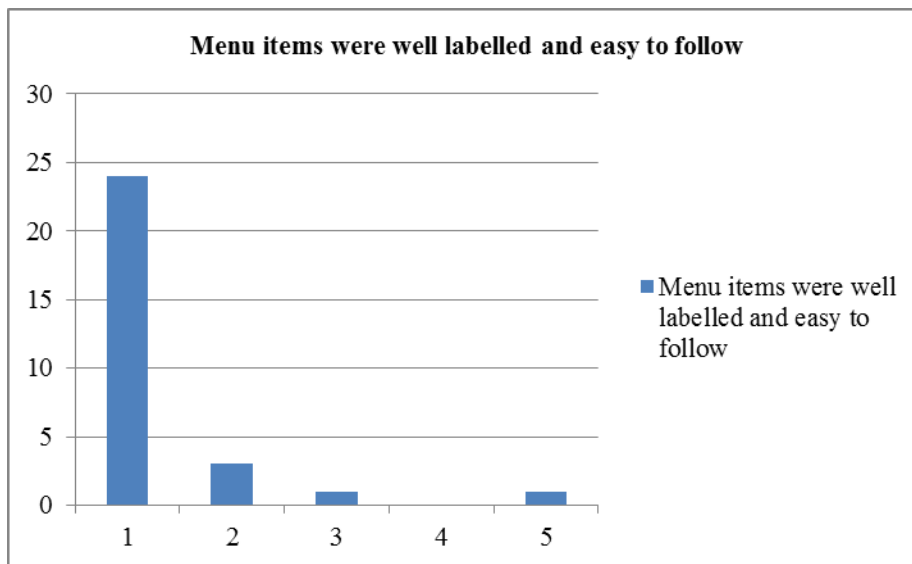
Figure 67 - The menu items were well labelled and easy to follow

Statement 12: *Navigation links allow quick access to various functionalities*

All the police officers in the study replied to this statement. Most of them strongly agree (23), five agreed (5) while one respondent remained neutral (1) to this statement.
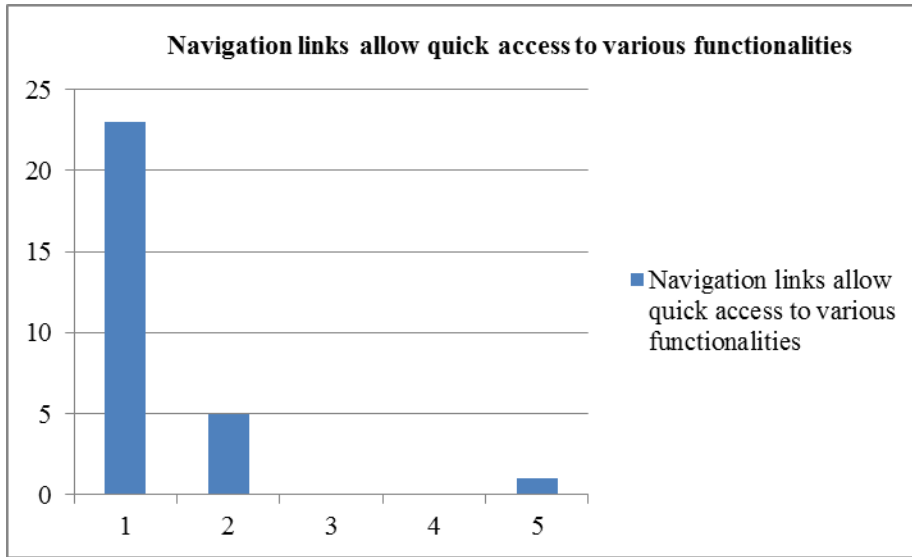
Figure 68 - Navigation links allow quick access to various functionalities

Statement 13: C*onsistent page structure in all web interfaces*

All the police officers in the study replied to this statement. Most of them strongly agree (22), four agree (4), one strongly disagrees (1). Two respondents remained neutral (2) to this statement.
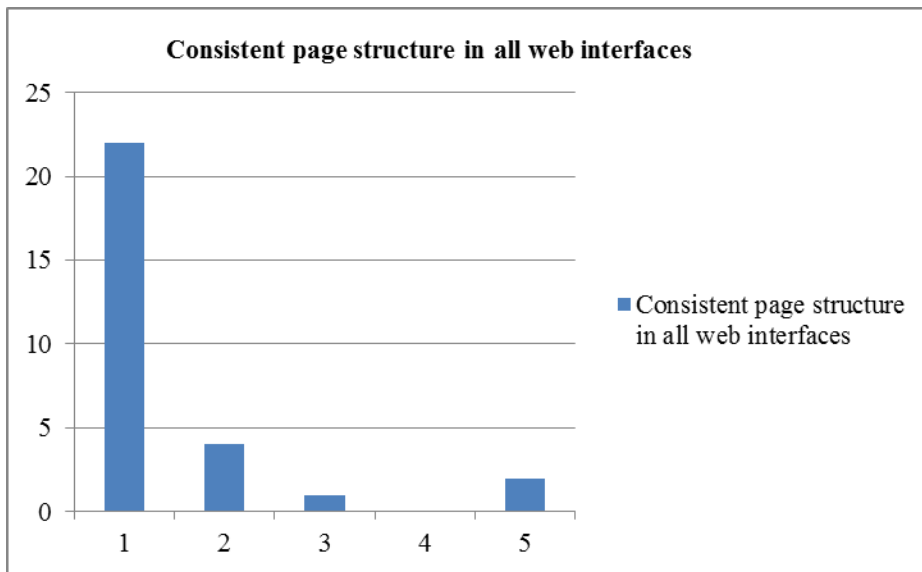
Figure 69 - Consistent page structure in all web interfaces

Statement 14: *There were adequate access control mechanisms to ensure only registered users can access the system*

All the police officers in the study replied to this statement. Most of them strongly agree (22), six agree (6) while only remain neutral (1) to this statement
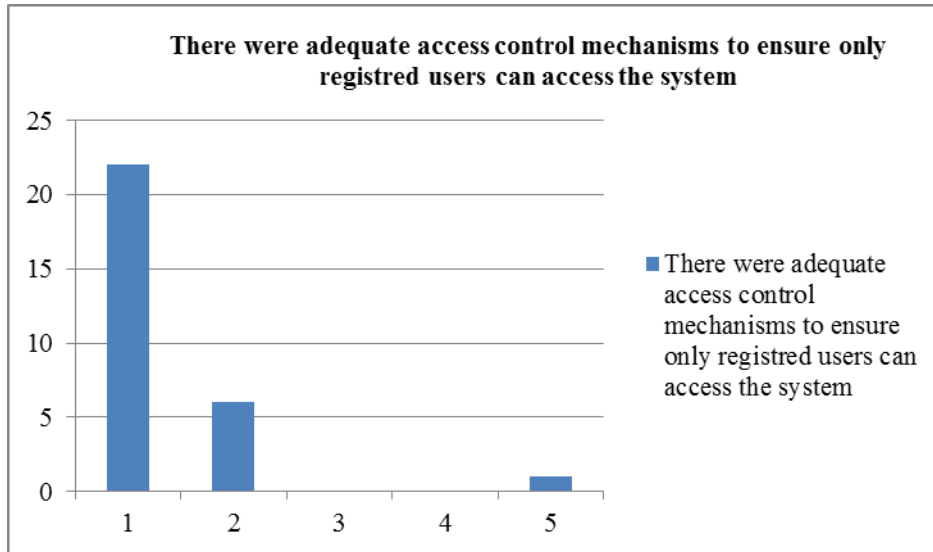

Figure 70 - There were adequate access control mechanisms to ensure only registered users can access the system

6.3 CHAPTER SUMMARY

This chapter has provided a summary of the results and a brief discussion on the research instrument used.

5.0 ACHIEVEMENTS, EVALUATION AND FUTURE WORK

This section shall use the achievements of the two objectives laid down during the project proposal and the analysis done to synthesize a set of recommendations for Nairobi Police security enhancement via the usage of an SMS gateway.

5.1 ACHIEVEMENTS

Under objective one, the project was "To study the current communication means used by the police and the general public, identify the gaps in the communication and if technologies like SMS gateway might be a solution for these gaps". In the intervening study, it was established that most police officers and members of public owned mobile phones and had long experience on SMS usage on a daily basis. Despite mobile phone and SMS usage on daily basis, police officers and members of the public mostly use face to face communication which is slow, manual and inconvenient in information flow. The study established that SMS communication (sending/receiving) between the members of the public and the police was very rare. The same case applied to the intra-police SMS communication.

Under objective two, the project was "To carry out the research on the limitations and challenges that might arise in the process of planning to implement and use an SMS gateway technology in the police setup for the purpose of security enhancement." In this study, members of the public managed to easily send SMS to police stations. The police officers also managed to easily communicate internally via the SMS gateway as well as send SMS to the members of the public. In terms of ease, convenience, speed and user friendliness in the processes of communicating security alerts, the system received high ratings from the members of the public as well as from the police officers. The only challenge / limitation was on the billing mechanism for the SMS line since this can only be addressed in an SMS gateway in the production environment and not at a prototype level like in this study.

4.1 EVALUATION OF THE STUDY

The purpose of the study was to study the usage of an SMS gateway in police setup with the aim of enhancing security. In telecommunication industry an SMS gateway is defined as a network facility for sending or receiving Short Message Service (SMS) transmissions to or from a telecommunications network that supports SMS. Most messages are eventually routed into the mobile phone networks.

This purpose was discussed in the introduction part, main objectives of this study were:

Objective 1: To study the current communication means used by the police and the general public, identify the gaps in the communication and if technologies like SMS gateway might be a solution for these gaps.

Objective 2: To carry out the research on the limitations and challenges that might arise in the process of planning to implement and use an SMS gateway technology in the police setup for the purpose of security enhancement.

All of these objectives were attained by this project.

First the introduction and literature review part of this study identified the insecurity and communication problems that are currently experienced by members of the public and the police officers. The motivation of usage the usage of an SMS gateway gathered great support with the high ownership of mobile phones and usage of SMS in daily communication. As shown by the study, if communication between the members of the public and the police is improved via the usage of this gateway, security as well will be improved due to the ease, convenience and speed experienced.

SMS gateway usage in communication is still in early phases of development. This study's focus on communication between the police and the members of the public via an SMS gateway has illustrated that it is possible to permit interactions for various groups for the sake of enhancing security.

The results of this study have demonstrated that the member of the public and the police generally use SMS on daily basis. Alongside that, the usage of an SMS gateway has demonstrated that it can provide a platform for the easy, convenient and reliable point of relying alert messages between members of the public and the police. It has also been seen that intra police communication is enhanced via this gateway as compared to the traditional use of other means like radio calls where some officers might be left out in the communication loop.

On the SMS gateway, all mobile phone numbers of the officers are stored in the database. Various groups created ensure messages are channelled to only concerned parties.

With only a single mobile number, the study has demonstrated that members of the public can be able to send SMS to a police inbox for example by starting all messages with "@langata" to send an alert to Langata police station, "@buruburu" to Buruburu etc. Due to this segmentation a single SMS line can be used to serve the whole Nairobi without the need of having each police station / post with its separate SMS line. This will avoid confusion about the phone numbers to use by both the police and members of the public for reporting purposes.

The study has also shown that all the incoming and outgoing SMS are stored in the database and can be used in the future by the police for reference e.g. gathering intelligence / data mining etc.

4.2 FUTURE WORK

Since SMS gateway is a still new area under research, further research can be carried out with the following objectives:

- To study and further design of the gateway to avoid the members of the public from misleading the police via the gateway e.g. false SMS. Mechanisms such as location based systems like Google maps need to be integrated with an SMS gateway to help identify SMS sources.

- The study should also focus on the creation of priority inboxes to ensure filtering of key words that might help officers pay attention mostly to.

- To follow up on a payment model. This needs to be agreed on with the both the internal security ministry and the mobile network operators so as to make it possible that SMS senders and recipients are not be charged by the mobile network operators.

REFERENCES

Abdel-qader et al. (2011) Using Short Message Service (SMS) to support business continuity. *World of Computer Sciennce and Information Technology Journal (WCSIT)*. P. 34-38.

Aizinezhad, M., Hashemi, M. (2012) The Pedagogical Applications of Using Short Message System (SMS) in language Learning Classes. *International Journal of Academic Research in Progressive Education and Development*, Vol 1, No. 1.

Ambani et al. (2012) Automatic Ticket Vending via Messaging Service (ATVMS). *International Journal of Computer Applications*. Volume 42– No.17.

Bose et al. (2010) SMS advertising and its prospects in Bangladesh. *Journal of Theoretical and Applied Technology*.

Brown, J., Shipman, B., Vetter, R. (2007) SMS: The Short Message Service.

Clicktell. (2012) 101 business applications using SMS. Clickatell.

Daily Mail. (2010) *Police told to send text messages because it is too expensive to speak on their radios*.[Online] Available from: http://www.dailymail.co.uk/news/article-1329538/Police-told-send-text-messages-expensive-speak-radios.html [Accessed: 1st September 2013].

Densmore, M. (2012) Experiences with bulk SMS for health financing in Uganda. *ACM*, May 5-10.

Ejnioui etal. (2012) Software architecture and prototype for supporting medical prescription adherence using SMS services. *Computer Technology and Application*.

Fedoraproject.org, computer software 2013. Available from: https://fedoraproject.org/ . [Accessed: 1st September 2013].

Furuzawa, Y. (2011) Two police reforms in Kenya – Their implications for police reform policy. *Journal of International Development and Cooperation*. Vol. 17, No.1, p. 51-69.

Hughes. (2013) AT Command Reference. [Online] Available from: http://www.hughes.com/AT_Command_Reference.html [Accessed: 14th September 2013].

Jadhao et al. (2012) Campus short message service system - classifying SMS effectively. *International Journal of Computer Applications(IJCA)*. p.15-17.

Kannel.org, computer software 2013. [Online] Available from: http://www.kannel.org. [1st September 2013].

Kaur et al. (2012) Wireless application. Proceedings of 'I-Society 2012' at GKU, Talwandi Sabo Bathinda (Punjab). *International Journal of Computing & Business Research*.

Kenya Police. (2013) *Police Contacts*. [Online] Available from: http://www.kenyapolice.go.ke/police%20hotlines.asp [Accessed: 1st September 2013].

LAPD. (2013) Los Angeles Police Department(LAPD) Anonymous Crime Tip Program Public Fact Sheet , CA, USA. [Online] Available from: https://www.google.co.tz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCwQFjAA&url= http%3A%2F%2Fwww.lapdonline.org%2Fget_informed%2Fpdf_view%2F39390&ei=JA0OU6mUD4-07QakloFo&usg=AFQjCNG5FCBcBMexTib_qwm-UyV6nxEizA&bvm=bv.61965928,d.ZGU [Accessed: 14th September 2013].

Mariadb, computer software 2013. [Online] Available from: https://mariadb.org . [Accessed: 1st September 2013].

Meng et al. (2011) Analysis of the Reliability of a Nationwide Short Message Service.

Mysql.com, computer software 2013. [Online] Available from: http://www.mysql.com/ [Accessed: 1st September 2013].

Perry, D. (2012) German Police Used 440K+ Stealth SMS to Track Suspects. [Online] Available from : http://www.tomsguide.com/us/cellphone-security-germany-sms-stealth,news-13717.html [Accessed: 1st September 2013].

Playsms.org, computer software 2013. [Online] Available from: http:// playsms.org . [Accessed: 1st September 2013].

RPP. (2012) Your guide to: The National Police Service act, The National Police Service Commission act and The Independent Policing Oversight Authority Act.

Sbaa, A. (2012) An SMS-SQL based On-board system to manage and query a database. *International Journal of Advanced Computer Science and Applications(IJACSA)*. Vol 3, No 6.

Scornavacca et al. (2007) Developing a SMS-based classroom interaction system. *MoLTA*.

Security Research and Information Center (SRIC). (2012) An overview of crime incidents in Nairobi region, Nairobi.

Standard Media. (2013) *Communication Commission of Kenya, police ordered to restore 999 emergency number*. [Online] Available from

http://www.standardmedia.co.ke/?articleID=2000088025&story_title=communication-commission-of-kenya-police-ordered-to-restore-999-emergency-number&pageNo=2 [Accessed: 1st September 2013].

Streicher, P. (2010) The role of SMS in the law. *PROLOG*. [Online] 10th December 2010. Available from http://www.prlog.org/11140507-the-role-of-sms-in-the-law.html [Accessed: 1st September 2013].

Susanto et al. (2008) A six-level model of SMS-based eGovernment. *International Conference on E-Government (ICEG)*, Oct 23-24.

Susanto et al. (2012) Deliverying public service via SMS: Types of the services and the acceptance factors.

Susanto, T, D and Goodwin, R. (2010) Factors Influencing Citizen Adoption of SMS-Based e-Government Services. *Electronic Journal of e-Government.* Volume 8 Issue 1 2010, p55 - 71.

Talukder, A.,Ahmed, H., Yavagal, R. (2010) *Mobile Computing – Technology, Applications and Service Creation*, 2nd ed., New Delhi: Prentice Hall.

Tan et al. (2009) Automatic power meter reading system using GSM network. *The 8th International Power Engineering Conference (IPEC)*.

The Open Source Initiative. (2013) The Open Source Initiative. [Online] Available from: http:// http://opensource.org/ [Accessed: 14th September 2013].

The Usalama Reforms Forum. (2012) Police reforms monitoring project – preparedness of the police to combat insecurity and crime, Nairobi.

Traynor et al. (2008) Exploiting open functionality in SMS-capable cellular networks. *Journal of Computer Security*, p713-742.

Tutorials Point. (2013) GSM Tutorial. [Online] Available from http://www.tutorialspoint.com/gsm/index.htm [Accessed 1st September 2013].

Zareen, et al. (2011) Mobile Computing-Architecture, Challenges and Research Isssues. *International Journal of Information Theory*, p5-8.

APPENDIX A: GENERAL PUBLIC QUESTIONNAIRE

SMS System (Gateway) usage by member of the public for security enhancement

INSTRUCTIONS

1. The aim of this study is to find out what you think of SMS sending / receiving via an SMS System (gateway) in order to enhance security.
   There is no correct or incorrect answer, give the best possible answer as per your understanding.

2. Your information and answers will not be shown to anyone else.

3. Read the statements carefully: use ✓ or ✗ for marking your response.

4. The questions in this questionnaire are close ended.

5. You may find some of the questions to be repeated in different sections of the questionnaire. This is to assist in the analysis of the research.

6. Please answer all questions.

SECTION A – Personal Information

1. Gender: ☐ Male ☐ Female

2. Occupation:_____
   _____

3. Estate:_____
   _____

SECTION B – Technological Background Details

1. Do you own a mobile phone? ☐ Yes ☐ No

2. How long have you used mobile phone?

   ☐ Never ☐ Less than 1 year ☐ 2-4 Years ☐ 5 years and above

3. Do you use SMS daily?

   ☐ Yes ☐ No

4. How many times do you use SMS (Short Message Service) daily?

   ☐ Never ☐ Less than 1 hour ☐ 1-2 hours ☐ 5 hours and above

5. How many years have you been using SMS (Short Message Service)?

☐ Never ☐ Less than 1 year ☐ 2-4 Years ☐ 5 years and above

6. Have you ever reported an incident or communicated to the police?

☐ Yes ☐ No

7. Which means do you use to communicate to the police?

☐ Landline Telephone ☐ Mobile call ☐ SMS ☐ E-mail ☐ Face to face ☐ Radio call ☐ Other

8. Have you ever reported an incident or communicated to the police using your mobile device?

☐ Yes ☐ No

9. Have you ever sent an SMS to a police station?

☐ Yes ☐ No

10. Have you ever received an SMS from a police station?

☐ Yes ☐ No

SECTION C –SMS System (Gateway) usage

Answer the next group of questions with Strongly Agree, Agree, Disagree or Strongly Disagree.

1. It is easy to send SMS from the SMS System (gateway).

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

2. It is easy to receive SMS from the SMS System (gateway) using mobile phone.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

3. I can get SMS from the SMS system anywhere and anytime I want using the SMS system.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

4. It is more convenient to send important alerts to the police using the SMS system.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

5. It is more convenient to receive important alerts from the police using the SMS system.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

6. It is possible to provide alert information to police using the SMS system.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

7. It is possible to receive alert information from police using the SMS system.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

8. It is possible to increase security measures by using SMS to report to the police

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

9. Sending SMS using the system did not take long

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

10. Receiving an SMS using the system did not take long

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

11. The menu items were well labelled and easy to follow.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

12. Navigation links allow quick access to various functionalities.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

13. Consistent page structure in all web interface

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

14. There were adequate access control mechanisms to ensure only registered users can access the system.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

Thank you for completing this survey. I really treasure your input and effort you made.

APPENDIX B: POLICE OFFICERS QUESTIONNAIRE

SMS System (Gateway) usage by the police officers for security enhancement

INSTRUCTIONS

7. The aim of this study is to find out what you think of SMS sending / receiving via an SMS System (gateway) in order to enhance security.
There is no correct or incorrect answer, give the best possible answer as per your understanding.

8. Your information and answers will not be shown to anyone else.

9. Read the statements carefully: use ✓ or ✗ for marking your response.

10. The questions in this questionnaire are close ended.

11. You may find some of the questions to be repeated in different sections of the questionnaire. This is to assist in the analysis of the research.

12. Please answer all questions.

SECTION A – Personal Information

4. Gender: ☐ Male ☐ Female

5. Occupation:_____
   _____

6. Estate:_____
   _____

7. Police Division:

   ☐ Buru Buru ☐ Central ☐ Embakasi ☐ Gigiri ☐ Kasarani ☐ Kilimani ☐ Langata

SECTION B – Technological Background Details

11. Do you own a mobile phone? ☐ Yes ☐ No

12. How long have you used mobile phone?

   ☐ Never ☐ Less than 1 year ☐ 2-4 Years ☐ 5 years and above

13. Do you use SMS daily?

   ☐ Yes ☐ No

14. How many times do you use SMS (Short Message Service) daily?

☐ Never ☐ Less than 1 hour ☐ 1-2 hours ☐ 5 hours and above

15. How many years have you been using SMS (Short Message Service)?

☐ Never ☐ Less than 1 year ☐ 2-4 Years ☐ 5 years and above

16. Which means do you use mostly to communicate to the other police officers in relation to work matters?

☐ Landline Telephone ☐ Mobile call ☐ SMS ☐ E-mail ☐ Face to face ☐ Radio call ☐ Other

17. Which means do you use mostly communicate to the member of the public?

☐ Landline Telephone ☐ Mobile call ☐ SMS ☐ E-mail ☐ Face to face ☐ Radio call ☐ Other

18. Have you ever reported an incident or communicated to the other police officers using your mobile device?

☐ Yes ☐ No

19. Have you ever sent an SMS to a police station?

☐ Yes ☐ No

20. Have you ever received an SMS from a police station?

☐ Yes ☐ No

SECTION C –SMS System (Gateway) usage

Answer the next group of questions with Strongly Agree, Agree, Disagree or Strongly Disagree.

15. It is easy to send SMS from the SMS System (gateway).

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

16. It is easy to receive SMS from the SMS System (gateway) using mobile phone.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

17. I can get SMS from the SMS system anywhere and anytime I want using the SMS system.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

18. It is more convenient to send important alerts to other police officers using the SMS system.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

19. It is more convenient to receive important alerts from the other police officers using the SMS system.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

20. It is possible to provide alert information to police using the SMS system.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

21. It is possible to receive alert information from police using the SMS system.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

22. It is possible to increase security measures by using SMS to report to the police using the SMS system

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

23. Sending SMS using the system did not take long

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

24. Receiving SMS using the system did not take long

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

25. The menu items were well labelled and easy to follow.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

26. Navigation links allow quick access to various functionalities.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

27. Consistent page structure in all web interface

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

28. There were adequate access control mechanisms to ensure only registered users can access the system.

☐ Strongly agree ☐ Agree ☐ Strongly Disagree ☐ Disagree ☐ Neutral

Thank you for completing this survey. I really treasure your input and effort you made.

APPENDIX C: LETTER OF TRASMITTAL

<div align="right">

Duncan O. Mwamba

University of Nairobi

duncan.owino@gmail.com

Cell phone: 0738 967 285

</div>

Dear respondent,

I am a master's student of the University of Nairobi in the School of Computing and Informatics and undertaking research on the police security enhancement via an SMS gateway usage. The aim of this research is to get police and the public perception on usage of an SMS gateway to enhance communication between the police and general public for the sake of improving the current security state. This study forms a major component of the requirement for the fulfilment for the degree of Master of Science in Information Systems.

In order to produce the required information, you are humbly requested to respond honestly and objectively to all the items in the questionnaire guide to the best of your knowledge.

Please do not enter your name or contact details on the questionnaire. It remains anonymous. Information provided by you remains confidential and will be reported in summary format only.

Should you have any queries or comments regarding this survey, you are welcome to contact me

Kind regards,

Duncan O. Mwamba

APPENDIX D: INSTALLATION AND CONFIGURATIONS OF THE SMS GATEWAY

1.1 Installing the gateway

Step 1: The latest source of kannel for production was downloaded from http://www.kannel.org/download.shtml

Kannel version 1.5.0 downloaded and used for this project

Step 2: After unpacking the source package, we need to compile the gateway as follows:

#./configure

#make

The *configure* script investigates various things on your computer for the Kannel compilation needs and writes out the Makefile used to comple Kannel. **Make** then runs the commants to actually compile Kannel.

Step 3: after compiling the gateway, we need to install certain programs in a suitable place. This is done using make again. i.e.

#make install

The programs that are installed are (as filenames from the root of the source directory):

gw/bearerbox

gw/smsbox

gw/wapbox

The version number of the gateway is added to the filenames during installation.   This makes it easier to have serveral versions installed and makes it eary to go back to an old version if the new version proves problematic.

1.1.1   Configuring the gateway

Our Kannel is going to be configured as SMS gateway. WAP gateway functionality is not going to be configured.

1.1.1.1   – Bearer Box Configuration

The **bearerbox** consists of two groups:

- 'core' group

- 'smsc' group

i.e. The bearer box configurations will be:

#--------------------------------------CORE GROUP--#

119

group = core

admin-port = 13000

smsbox-port = 13001

admin-password = bar

#status-password = foo

admin-deny-ip = "*.*.*.*"

admin-allow-ip = "127.0.0.1"

log-file = "/var/log/kannel/bearerbox.log"

log-level = 0

box-deny-ip = "*.*.*.*"

box-allow-ip = "127.0.0.1"

access-log = "/var/log/kannel/access.log"

store-file = "/var/log/kannel/kannel.store"

#THIS DEFINES EXTERNAL DLR STORAGE

dlr-storage = internal

#--SMSC GROUP---#

group = smsc

smsc = at

modemtype = auto

device = /dev/ttyACM0

my-number = 3543870236903270

smsc-id = kepolice

log-level = 0

log-file = "/var/log/kannel/smsc.log"

log-level = 0

sim-buffering = true

#--MODEM GROUP---#

group = modems

id = Sony Ericsson

name = "Sony Ericsson C702"

detect-string = "Sony"

#init-string = "ATZ"

#init-string = "ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0"

init-string = "AT+CNMI=2,0,0,0"

message-storage = "ME"

#---#

1.1.1.2 – SMS Box Configuration

The **smsbox** consists of two groups:

- − 'sms-service' group

- − 'sendsms-user' group

We shall use the following configurations:

#-------------------------------------SMSBOX GROUP--#

group = smsbox

bearerbox-host = 127.0.0.1

sendsms-port = 13013

global-sender = "+254735922584"

log-file = "/var/log/kannel/smsbox.log"

log-level = 1

#---SENDSMS-USER GROUP--#

group = sendsms-user

username = tester

password = foobar

concatenation = true

max-messages = 0

#--SMS-SERVICE GROUP--#

group = sms-service

keyword-regex = .*

catch-all = true

max-messages = 0

catch-all = true

#--#

Note: all the bearerbox and smsbox configurations will be stored in /etc/kannel.conf file

1.1.2 Running the gateway

Bearebox and smsbox should be always started by the superuser (root user).

First start with the bearerbox followed by the smsbox using the below commands as root user:

#bearerbox –v 1 /etc/kannel.conf &

#smsbox –v 1 /etc/kannel.conf &

Confirm the status of kannel using the below command:

#lynx –dump http://localhost:13000/status

Or running the same URL on a browser

4.2.1 Installing and configuring playsms

The steps to install playsms:

Step 1: Create a UNIX user named 'playsms' to manage playsms i.e.

#adduser playsms

#passwd playsms

Step 2: we shall create a directory for this users web files and assign it ownership to playsms i.e.

#mkdir /var/www/playsms

#chown playsms /var/www/playsms

Step 3: as root user extract playsms package in /usr/local/src i.e.

#tar –zxvf playsms-x-x-x.tar.gz –C /usr/local/src

#cd /usr/local/src/playsms-x-x-x

Step 4: we shall copy 'web' directory to /var/www/playsms and set owner back to user playsms i.e.

#cp –rR web/* /var/www/playsms

#chown –R /var/www/playsms

#chmod 701 /var/www/playsms

Installing MYSQL, APACHE , PHP and PHP PEAR DB

Step 1: install MySQL I,e,

#yum install mysql

Step 2: install MySQL-server

#yum install mysql-server

Check daemon status:

#service mysqld status

#chkconfig –levels 235 mysqld

#service mysqld start

Step 3: install Apache

#yum install httpd

#service httpd status

Test if apache is running. Type the url in a browser:

http://localhost

Step 4: Install PHP

#yum install php

Restart apache:

#service httpd restart

Step 5: test if PHP is properly installed. Create and test phpinfo.php web page:

#vi /var/www/htmp/phpinfo.php

<?php

       Phpinfo()

?>

CTRL+D

Test the above page: http://localhost/phpinfo.php or lynx -dump "http://localhost/phpinfo.php"

Step 5: enable PHP to connect to mysql:

#yum install php-mysql

Restart httpd

You shole see mysql enable on phpinfo.php

Step 5: Install PHP PEAR DB

#yum install php-pear-DB

Step 6: Import database

#mysqladmin –u root –p create playsms

#mysql –u root –p playsms < /usr/local/src/playsms-x-x-x/db/playsms/sql

Step 7: confirm playsms tables are created

#mysql –u root

Mysql > show database;

Mysql > show playsms;

Mysql > show tables;

Mysql> quit;

Step 8: edit /var/www/playsms/config.php to make the database password to be null.i.e.

$db_param['pass'] = '';

Step 9: test php-mysql db connection works. Create a database test web page:

#vi /var/www/dbtest.php

<?php

$link = mysql_connect ('localhost', 'root', '');

If (!$link) {

Die ('could not connect: ' . mysql_error());

}

Echo 'connected successfully';

Mysql_close($link);

?>

Test the webpage: http://localhost/dbtest.php

Step 10: copy playsmsd and playsmsd_start to /usr/local/bin

Step 11: as root user:

Cp –pr /var/www/playsms /var/www/Nairobi-police-sms

4.2.2   Running playsms

To start playsms:

http://localhost/nairobi-police-sms

username: admin

password: admin