International Journal of Computer Applications (0975 - 8887)
Volume 169 - No.8, July 2017

Automatic Security Monitoring and Alert System through Sound Analysis

Daniel Isoso Machanje
Faculty of Information Technology,
Strathmore University
P.O Box 59857-00200
Nairobi, Kenya

Joseph Onderi Orero
Faculty of Information Technology,
Strathmore University
P.O Box 59857-00200
Nairobi, Kenya

ABSTRACT

Insecurity is a common scenario, especially in developing countries such as Kenya, where many households and institutions are accountable of their own security, forcing them to implement manual processes of securing their surroundings. These manual means include the deployment of untrained and ill-equipped security personnel, who barely have any skills to combat any potential criminals.
There is a need to introduce an automatic means of monitoring and recognition within the vicinity of an environment in cases of criminal and distress scenarios. Such a system will be able to eliminate the physical placement of security guards within a vicinity, thus improving personnel privacy and reducing expenses while at the same time, increasing effectiveness with regard to security monitoring and alerting in case of incidences.
In this study, an Automatic Security Monitoring and Alert System through Sound Analysis is proposed. The proposed system will be able to monitor the vicinity through sound analysis, and be able to broadcast an alert in case of a security breach. The system will be able to detect sound variations in the environment and alert security agents on the other end, who will respond to the emergency. An automatic analysis of sound, that will include abnormal sound variations based on the pitch measured in decibels on the client's end of the listened sound will be responsible for determining the need for triggering the system into action.
A mobile application was developed to facilitate the demonstration of the proposed solution, gaining an acceptability rate of 84% by the users.

Keywords

Security, Automatic, Sound, Mobile, Monitoring, Alert

1. INTRODUCTION

Crime rates, both locally and internationally, have been a rising concern for security bodies and citizens at an equal level. The lifestyle quality of most households have been hampered while security officers have been incapacitated in dealing sufficiently with the soaring crime rates. The incapacity of security bodies to uphold the security and safety concerns of citizens in developing countries could be attributed to the few number of police forces. For instance, in Kenya, the police to population ratio according to the last study, stands at 1:1150, which is way too below the UN-recommended 1:450 ratio [4].
Households and institutions have opted to source security from privately owned security agencies which stand in their hundreds in developing countries, as they serve as a key employment body. However, the restrictive weaponry and tools that these security agencies suffer has left them barely able to contain the crime rates experienced in households and institutions they guard. Criminals have taken the advantage of their unequipped state to find ways of evading detection and holding the security guards hostage while they go on the criminal activities. Despite this, many institutions still emphasize on their need of these security agencies given the desperation that exists on the need for security.
This paper documents the scope of an Automatic Security Monitoring and Alert System through Sound Analysis that relies on the trigger of certain sound decibels in the surrounding environment to trigger a background-running application that will transmit the triggers either to a security agency or other personal helps. These trigger alert messages, sent after a certain trigger threshold is attained, constitute an automatic message that gives a general possibility of danger, an exact location from where the message will be sent by the use of the mobile phone number, and a time-stamp that will indicate the time of the trigger. The locations of the trigger will be published on a map using Geographical Positioning System (GPS) initially saved by the homeowner.
Sound and voice recognition is an aspect of Natural Language Processing (NLP) that implements a way in which machines can learn and interpret voice to trigger programmed actions. This innovation has been vastly used in mobile devices to ease the way a user interacts with the device. Most current applications, especially under the Android regime, utilize voice recognition to give commands to applications, and speech recognition that is used to convert speech into text [3].
In this paper, sound recognition is utilized to trigger an application running in the background, unless turned off by the user. Through the mobile device's microphone, the application will be able to listen and monitor on certain voice amplitudes and convert the same to decibels (dB). A certain threshold reached will be regarded as a threat and will trigger the application to transmit an alert to responsible or set personnel that may include individuals or security agencies. The unique mobile numbers that each device has ensures quick location and reaction of different alerts in case of a need to

do the same by security agents with the help of GPS navigation that may have been initially mapped or drawn automatically by the application's capability in real time.
The proposed solution in this paper integrates the vital solutions of Natural Language Processing (NLP) in voice and sound recognition, message broadcasting and GPS services to implement an alert system for households that is triggered and broadcasted through a number of communication protocols by simply the detection of certain tonal amplitudes and decibels of the surrounding environment. A trigger will prompt the application to transmit the alert message with regard to the preference of the user of either sending the alerts periodically or when a certain threshold is reached. This innovation is aimed at the facilitation of a trigger system that will be of applicability in situations where the household users cannot access their phone devices. The impulse reaction by humans in drastic situations to produce high-pitched voices is the main motivation of this study. The application will also help eliminate the need of physically stationing security personnel within premises, limiting their presence only when necessary after an alert has been broadcasted.

2. LITERATURE REVIEW

2.1 Security in Developing Countries

Security is one of the key subject in developing countries that still has governments grappling at what actions to take to reduce criminal activities. Equally, developing countries face numerous threats too, especially at this age of terrorism. Criminals in developing countries have always thrived due to the incapacity that personnel and institutions face with regard to technologies to facilitate quick response. This could be attributed to the priority these countries give to other budgetary items which are weightier given the circumstances of the countries, such as health and education. Most developing countries have poor police to population ratio. For instance, Kenya has a police to population ratio standing at 1:1150. This, against the UN-recommended 1:450 ratio [4], draws the gap that exists in countries that mostly rely on physical placement of security forces to enforce security.

2.2 Security Agency Response Structure and Operation

Due to the deficiency that most developing countries have with regard to the police force, security agencies play a significant role in these countries' security. Most developing countries host a number of security agencies, each separate with their own governing and operational bodies. This trend can be attributed by the fact that these agencies are a huge employer of semi-illiterate populations that can not acquire formal education. A few security companies are internationally, providing trained personnel and a few modern equipment. A majority, however, have been locally formed by individuals lacking experience in the security sector. Institutions or homes are barely complete without an "askari" at the entrance of their premises. This existence can hardly escape anyone with an intention to implement any security innovation in the country; be it technological or otherwise [10].
The existence of security guards leased by most of the security agencies has, however, been put in questions in recent times, with most critics citing the frequent attacks on homeowners and individuals at public amenities. This has compromised the responsibilities that security agencies have in partaking their duties, with most trying hard to implement better strategies to combat security. Among these have been the deployment of more security guards, who despite the efforts, are still few; use of trained dog security; installation of sirens and alarms; and use of walkie-talkies for real time communication. In all these facets, the most current technology, mobile technology, has escaped discussion as a vital solution. All other industries seem to have embraced mobile technology in their implementations, save for security agencies [10].
Given the dynamism that security threats arise each day, coupled with the void in implementation of technology to counter insecurity among households and institutions, there is a need to develop more enhanced security applications using cheaply available and flexible mobile operating systems to monitor and give alerts on security breaches. Presently, there are a number of mobile-based security alert warnings most of which implement location-based technologies, but only after a prompt from the user. To avoid this scenario, a mobile application that will automate monitoring and automatically send alerts, either periodically or after a trigger given the preference of the user, is required. This would even help eliminate the need of security guards within households and institutions, limiting their presence in only the most needed scenarios or when alerted by mechanisms that will be implemented by the said mobile application.

2.3 Mobile use Penetration and Application in Security

2.3.1 Mobile penetration: Kenya and Globally. According to Kemibaro [6], Kenya had a 63% mobile penetration by the last quarter of the year 2012. This was projected to rise to 78% by 2017, which by current statistics according to the Communications Authority of Kenya (CAK), has surpassed the mark to stand at over 90% given the 2016 end year mark of 88.1%. This could be attributed to the infiltration of affordable smartphones in the market that was spearheaded by Android smartphones which retail for as little as $40. Globally, the growth rate of Android phones is placed at over 1.3 million activations per day.
Currently, there is an estimated mobile penetration of 6.8 billion, representing 96% of the world population, with a tremendous and varied growth rate ranging from 11% to 40% in various geographical locations through statistical studies [11].
The rising popularity of mobile phone technologies that have been implemented in many sectors of the economy, mostly health and commerce, have not been fully utilized in the security sector to promote security by incorporating technologies that would monitor and give feedback or react to certain triggers. Instead, many security agencies, who have been burdened with the responsibility to guard households and institutions given the wanting situation in the police force, have employed manual ways of implementing security that has left the ineffective and inefficient.

2.3.2 Mobile Implementation in Security. Various technological implementations to foster security have been in existence due to the efforts by some companies to incorporate automation in monitoring. Till recently, there have been many web-based solutions that were implemented through numerous communication and platform protocols to broadcast alert/warning messages [14]. One of the most recent progress in the Web sector was the Sensor Web, an intelligent system that utilized the Sensor Web Enablement (SWE) and Open Geospatial Consortium (OGC) tools for infrastructural framework implementation [5].
The technological sphere has, however, gradually shifted from PC-related solutions to the mobile platform given the vast mobile penetration that has taken the world by storm. This shift from PC to mobile has facilitated the innovation of many mobile platforms that include Android, Windows, Symbian, Badoo for old Samsung models, BlackBerry, and iOS. Among these, the most dynamic mo-

bile operating system is Android, and given its recent release to the market that dates back to about 9 years ago, the platform threatens the rest of the operating systems, with its major stronghold being its open source stature and cheap availability of many mobile handsets that support it [3].

The need for employing an innovative and automatic way of sending security alerts and notifications has never been this urgent. The contemporary world is filled with numerous security threats that arise from the fast-deteriorating virtues and social norms. The coincidental rise of mobile penetration currently at an astonishing 6.8 billion, a figure representing 96% of the current world population estimated at 7.5 billion creates an opportunity to create a viable solution to aid in security control and emergency response. Through the integration of several phone utilities and technologies, it is possible to come up with an application that would trigger a security alert at the onset of a security threat detection from sound monitoring. Many applications have already been created in regard to this with most implementing location-based technology, GPS, mapping technology, and message broadcasting protocols.

2.4 Review of Previous Research and Similar Applications

2.4.1 Thailand's Emergency Medical Service (EMS) Alert System. A study into the integration GIS and GPS technologies in handheld devices was implemented by Kowtanapanich, Tanaboriboon, and Chadbunchachai [7] in a bid to migrate from the traditional ways of recording accident data. A case study of Thailand's Emergency Medical Service (EMS) and the way data on accidents was collected provided a key benchmark in considering strategies in which GIS and GPS would be employed in hand-held devices to implement a less error-prone, standardized and efficient way of managing accident data collection and analysis. GPS provided a perfect platform to record spatial data describing the exact location of each accident (Bolstad, 2012). The GIS on the other hand, provided a platform for mapping previously mapped location and provide a database management that would facilitate data analysis, retrieval, and distribution. The role that the GIS played was especially of significance as the information gathered and recorded over time could be used in further studies to form strategies to enforce road safety in mapped areas. The main challenge encountered in feeding the GIS arose from reliable data acquisition and a mapping of the data accrued to appropriate policies and authorities that would provide remedies for the emergencies [7].

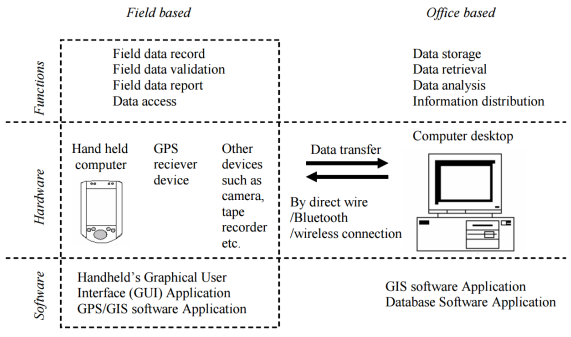

Fig. 1. Thailand's Emergency Medical Service (EMS) Alert System [7]

2.5 Sound and Voice Biometrics: Cross-Conversion of GIS Language with Chinese

The increasing demand from mobile device users for wireless location services has shifted a lot of focus on research related to location-based technologies. GPS and WLAN, the two main technologies that facilitate location positioning, have been compared to contain similar functionality with sometimes WLAN emerging a better technology due to some restrictions GPS faces in some operational environments featuring complex frameworks. Nevertheless, the utilization of positioning techniques; fingerprinting and triangulation, could both use speech recognition to facilitate the feeding of spatial data into GIS [2].

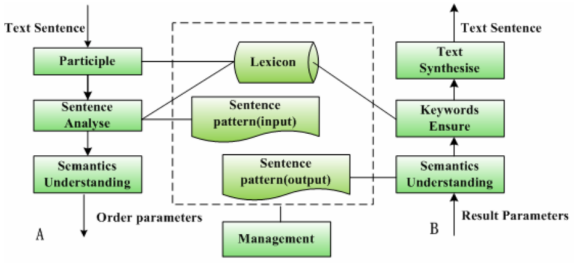

Fig. 2. The Cross-conversion of GIS Language with Chinese [2]

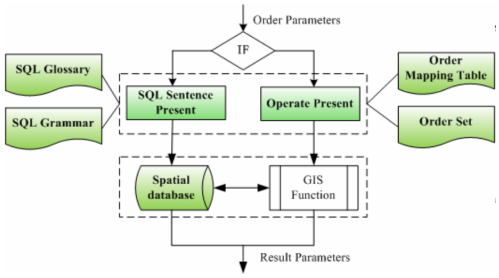

Fig. 3. The Command Parameter of GIS Manipulate Tool [2]

In recent years, mobile devices have faced technical limitations in implementing any voice biometrics courtesy of language complexity that exists in the multilingual world. More technicalities are experienced in the implementation of any voice functionality in more complex technologies such as GIS. In their study, Feng and Liu [2] justify the need of understanding geospatial information through normal, tactile feedback. The complexity involved in dealing with GIS tools, especially to device users that lack technical knowhow, could be made easier through the utilization of the voice. With a knowledge background provided by IBM's ViaVoice speech engine that made deep research into the integration of navigation systems and speech or voice technology, implementation of a GIS integrated with GPS and speech recognition was a viable venture.

2.6 Similar Applications

2.6.1 Armorvox. Voice biometrics and speech recognition are two technologies usually perceived as similar by many users, yet they are two aspects in the mobile world that are each unique to

the other [1]. Speech recognition is a technology that is incorporated in mobile devices to facilitate speech to text translation and simple voice commands to control and manipulate a device while voice biometrics comprise of special features about each unique voice that identifies the users to a registered system that has learnt to interpret each distinct voice and match it against identities.
The clear distinction that appears between the two aspects of voice technology need to be taken serious. Armorvox [1] identifies a flaw in voice biometric features that were implemented and configured using speech recognition technologies. The flaws involved may facilitate threats such as the lock-out of valid users and the intrusion of invalidated individuals. In order to ensure that effective and efficient voice applications are built, especially in the security sector, care is needed to calibrate the synthesis mode of each target platform in order to ensure quality checking to avoid false alarms and to facilitate a desired amount of automations.

2.6.2 Safety Notification Broadcast System. Ranganath [14] justifies the utilization of message broadcast in alert scenarios to foster safety to wireless mobile devices due to the widespread wireless coverage penetration. Enhancement of the broadcast is stamped by the inclusion of geographic areas that might be under threat, ensuring quick location and real-time emergency procedures triggered by the messages broadcasted at the onset of any security breach. Through these capabilities, Ranganath [14] proposes a means of designing network protocol supporting Android that could support the worthy cause of broadcasting safety notifications.
Mobile devices have a way of abstracting the backend processes such as operations by the Common Alerting Protocol (CAP), ensuring that the users are aware of the ultimate functionality by which mobile devices are able to identify the origin of a message, and furthermore, identify its purpose. Despite the inclusion of more technical location-based technologies here and GIS, there is clear testimony that through the correct prioritization, a mobile device is able to filter information being processed and perform its predefined functionalities, immediately notifying users of intended purpose, in that particular case being a need for emergency response [14].
Through the Android DDMS (Dalvik Debug Monitor Server), the Safety Notification Broadcast System (SNBS) has the capability of counterchecking repeated messages and deleting them to avoid any duplication. This is a great feature incorporated as it helps avoid the exhaustion of memory and the possibility of triggering false alarms especially preceding or succeeding a recent alarm that had earlier or would later trigger message broadcast [14].

2.6.3 Be Quiet. Be Quiet is an Android app that has the ability to listen to the environment of its vicinity, detect any noise, and alert the users by flagging a feedback message and an emoticon with color variations to indicate the levels of distress caused by noise. There is even an inclusion of an audio alert depending on the setting preferences of the user to notify them of the environment's noise [13].

2.7 Voice and Sound Biometrics in Mobile Technology

Mobile biometrics have advanced over time given the shift of technology from other standard technological implementations to mobile devices. Initially, biometrics was a reserve for security implementation. By security implementation, this refers to the ability of only biometrically certified personnel being able to access certain premises. Failure to contain these credentials meant no access at all. The shift to mobile technology has diversified the field into more intelligent applications, going over the initial stagnated application of biometrics [9].
Among the many biometric applications that mobile technology have ushered include visual (face) and voice biometrics. These two have facilitated a higher level interaction between humans and mobile devices, increasing both security and other applications by folds. The real-time feature of these biometrics has flattered the most ardent developers to venture into development of applications with such key features [15].

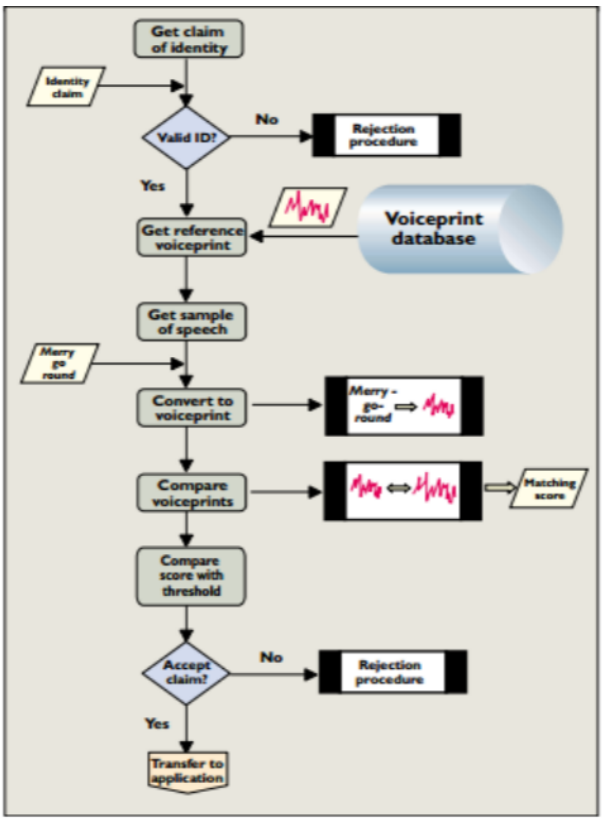

Fig. 4. A Model Implementing Voice Biometrics Security through Stored Models [15]

Mobile biometrics, both visual and voice have been known to work by computing feature vectors from the sources and directly comparing them against models initially stored into the system or against certain set thresholds. The feedback is always as a result of bimodal verification that reacts according to the matches that have been identified [15].

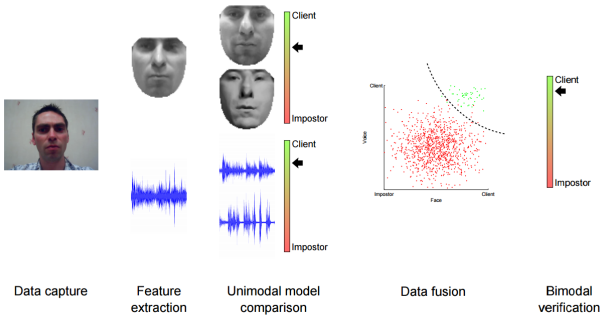

Fig. 5. Mobile (Sound and Visual) Biometric Verification [15].

The application of such mechanisms have been facilitated by the era of smartphones that have ushered in larger memory, processing, and features that include well placed cameras and microphones.
Voice detection and analysis is usually facilitated by the mobile's microphone, a component that captures the different voice variations in representations of voice tracts created by the sound frequency [8]. These tracts facilitate the use of a model, the Gaussian Mixture Model (GMM) to bring out clear analysis of a given sound, thus distinguishing the variously pitched voices to make sense for the purpose of analysis. This analysis sorts the noise in the voice from the actual sound to come up with segments of the sound to compare to either a stored model or a threshold before applying this against a certain application [15].
The changes made to the sound originally entered are accounted for using either the Z-norm formula:

$$z_q(y) = \frac{y - \mu_q}{\sigma_q}$$

or the Bayesian-based normalization technique formula:

$$P(q|y) = \frac{1}{1 + exp(-\alpha_q y - \beta_q)}$$

A graph, calculated using the said formulas could then be reproduced to show the errors experienced against certain threshold backdrops or stored voice models. This displays the error rate and margin that is accepted to avoid many false feedbacks to the system.

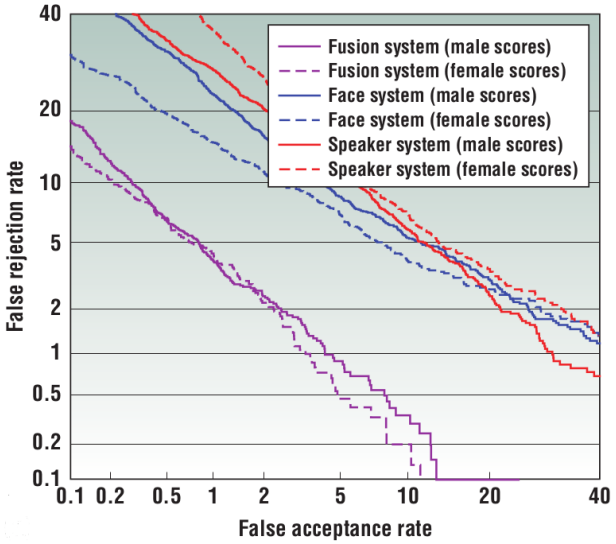

Fig. 6. Acceptable Error Rates by Z-norm or Bayesian Technique [15].

3. RESEARCH DESIGN, FINDINGS, AND IMPLEMENTATIONS

The scope of the study employed a number of research types that included descriptive research, explanatory research, qualitative research, and quantitative research.
With the study location set as Nairobi and its immediate vicinity, and given the foreseeable constraints and limitations in the scope of the study, a sample size population was be selected to reflect the feedback and observation of the rest of the population. For this purpose, two major sampling strategies were employed: stratified random sampling and rational subgrouping sampling [12].
Research instruments utilized to satisfy the research objectives included surveys in the form of interviews, questionnaires, documentation reviews, and other instruments of prototyping, and peer reviewers.

3.1 Data Analysis Procedures

Given the implementation of both qualitative and quantitative research methods, the data sampled and collected from the target population was analyzed with the use of SPSS. Other more objective analysis methods such as the Chi-square test and the ANOVA (Analysis of Variance) were also used to provide more conclusive information regarding various aspects of the study.

3.2 Findings and Discussions

3.2.1 Mobile Device Ownership. Before implementing a mobile solution, it was paramount to determine the accessibility of mobile phone devices among the potential user. Apart from only two respondents who reported loss of their phones as a result of theft, but still owned a cellphone courtesy of their friends, all the rest safely reported as having phones all the time. On this, it was a 100% ownership of mobile devices.

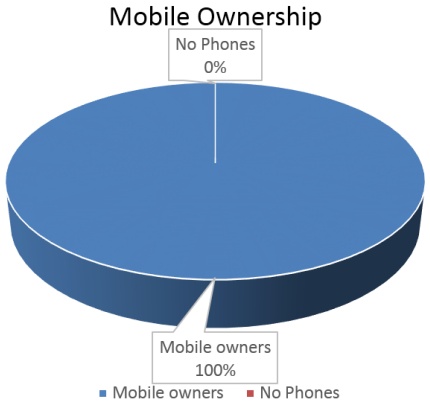

Fig. 7. Mobile Device Ownership

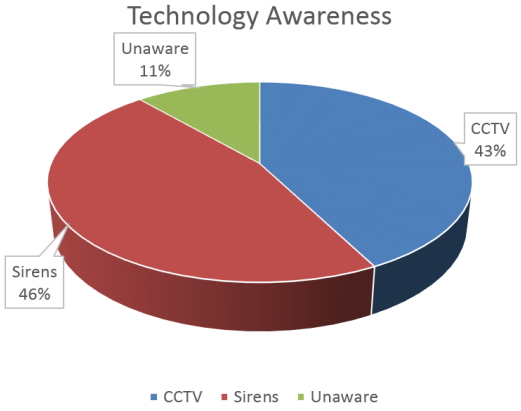

Fig. 9. Technology Awareness

3.2.2 Mobile Devices Operating System Popularity. In order to have a solid basis to select a mobile Operating system to develop the proposed solution, the first question asked among many was the type of phones they owned. A majority of the respondents; 99, had Android phones. Of the remaining, 18 owned windows phones, 9 owned iPhones, and the remaining 6 owned Symbian phones.

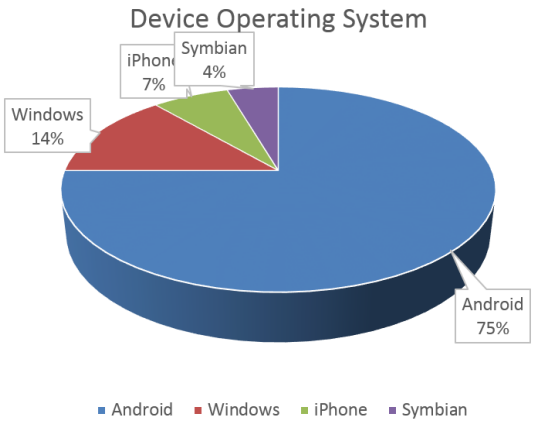

Fig. 8. Mobile Device Operating Systems

3.2.3 Awareness of Technologies used in Security Implementation. To find out the level of technological penetration in security measures and the awareness of the same by the respondents, a collection of the technologies known were asked. Of the total number, 56 were aware of CCTV camera usage, 61 were only aware of siren alerts, while the remaining number had no idea of any technology used apart from security guards.

3.2.4 Security Measure Implemented:. Given the state of security in the city and for the sake of finding out the most implemented security measure, the respondents were asked of the various security measures they had implemented in their home. 87 respondents mentioned Security guards from various agencies as their main security measures, 23 relied on dogs, 10 had installed alarms or sirens, and 12 had not implemented any security measures.

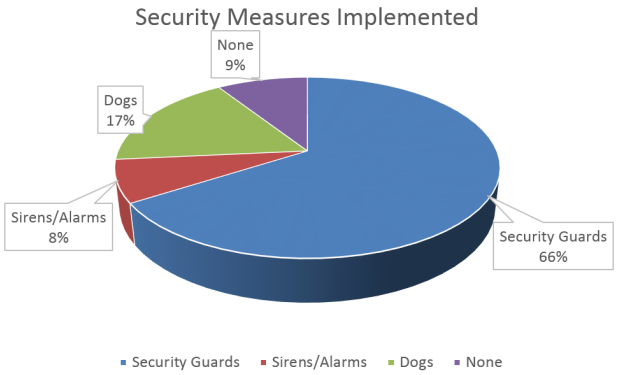

Fig. 10. Security Measures Implemented

3.2.5 Level of Confidence in Security Measures Implemented. With regard of each of the security measures implemented, each respondent was asked of the level of security they felt. A majority, 94, still felt insecure despite their implemented security measures. This was as a result of the declining state of security in the city. 13 of the respondents were confident of their security given their diverse security implementations, while the rest; 25, were unsure and left any future happenings to fate.

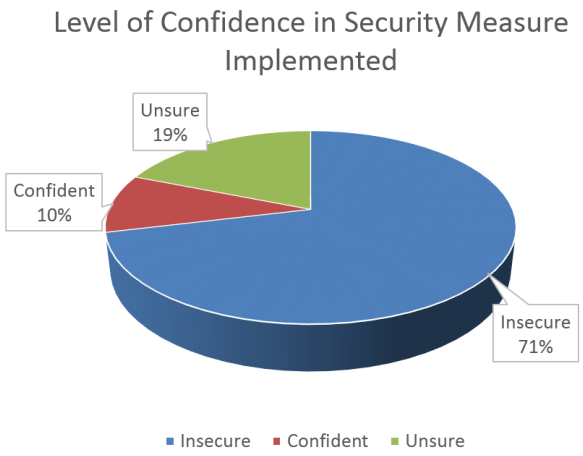

Fig. 11. Level of Confidence in Security Measure Implemented

3.2.6 Acceptability of a Mobile Solution. To find out the probability of the proposed solution's popularity, a question was asked to the respondents of their readiness in adopting a mobile security solution. 62 of the respondents were ready despite the costs associated, 41 admitted readiness but with the condition of no costs incurred, 16 declined citing confidence issues, and 13 were unsure of their decisions given the many available options for implementing security measures.

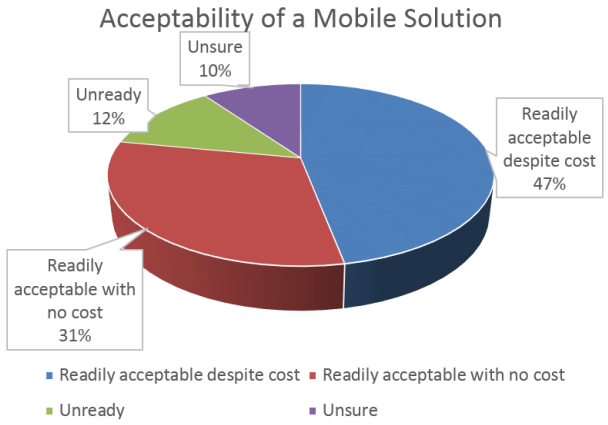

Fig. 12. Acceptability of a Mobile Solution

3.2.7 Favored Features for a Mobile Solution Application. The high rate of acceptability of a mobile solution prompted for higher levels of questions. Among the key questions to the respondents was the favored features to be implemented in terms of security monitoring. This was a closed end question with the given options to choose from including video, sound, and pictures. 89 of the respondents favored sound as the best trigger for alarm in a security situation. Most gave reasons of the lack of a need to access the phone in case of a security breach if this feature was to be used. They also cited the impulse reaction of noises in case of an attack. 26 of the respondents favored pictures citing their effectiveness of convicting in case of witness and proof needed in court cases, while 17 favored videos for the implementation of a mobile device security implementation.

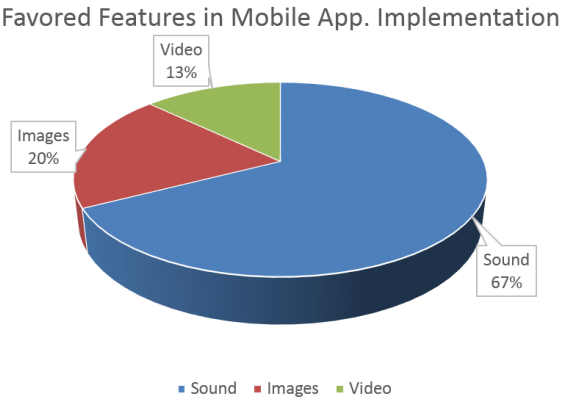

Fig. 13. Favored Features in Mobile App Implementation

3.2.8 Feedback Destination. Another closely related requirement of the proposed mobile solution that was asked was about the most preferred destination to where the feedback data of the recordings was to be sent. Given the provision that the services by Security Agencies would be paid for the purpose of response and follow up offered, while the feedback to close friends for response was free, there was a close range in the choices taken. 69 of the respondents chose feedback to Security Agencies given the constant monitoring they would offer and the guarantee of response, while 63 preferred feedback to friends due to the offer it gave of no charges.

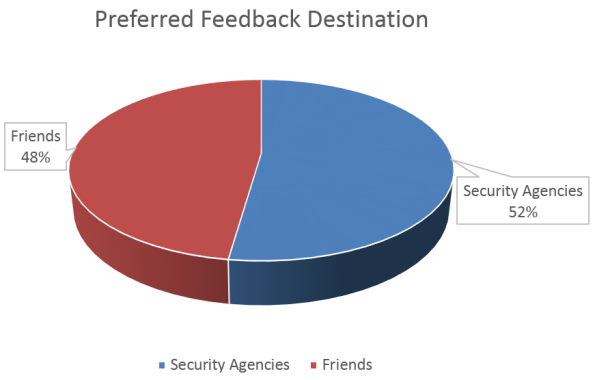

Fig. 14. Preferred Feedback Destination

3.2.9 Time Preference. Time preference was another key factor to be extracted from the users as it was key to know about the most preferred time that the proposed mobile solution would be needed. With two choice of night or day given, over 80% of the respondents chose night as the most appropriate time to use the said application. This constituted 113 of all the respondents. The remaining 19 respondents favored the day after being informed there was no choice of both night and day.

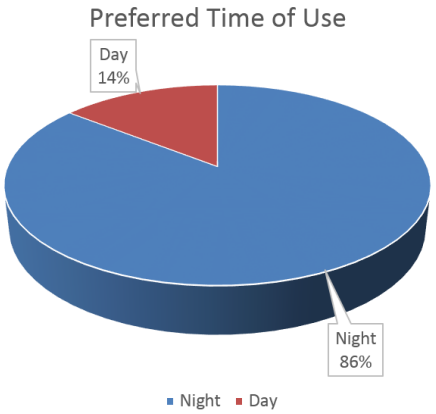

Fig. 15. Preferred Time of Use

3.2.10 Effort Put by Security Agencies in Implementing Technological Applications. In a bid to find out the effort and resources security agencies have invested to implement modern technology, a question was asked to some senior management personnel in a few security agencies. The question was structured in a way that directed the personnel to specify a percentage range of budget allocated for technological implementations. With a collection of 6 managerial personnel from three different security agencies asked, 2 said their budget dedicated between 14% and 22% of their budgets to technological innovations for security, 1 reported of a budget allocation of between 7% and 12%, while 3 reported of no budget allocations.

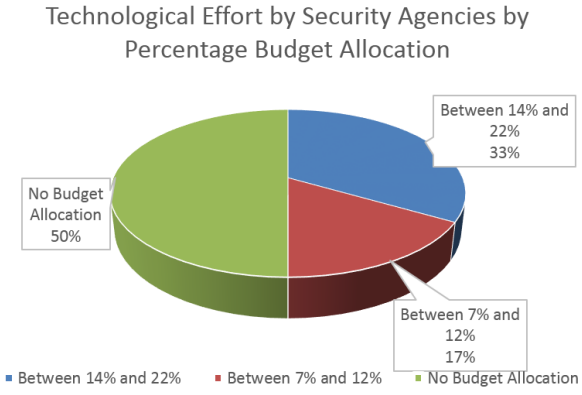

Fig. 16. Preferred Time of Use

3.2.11 Main Skill used by Security Guards in their Night Duty. To find out the most used skill in monitoring the security of a homestead in order to translate the same into the proposed application, a question was asked to a total of 20 security guards. Among these, 14 declared that keen listening was the first and key skill required especially in the quiet night environment. The rest of the guards favored visual observation as the key skill required for homestead monitoring.

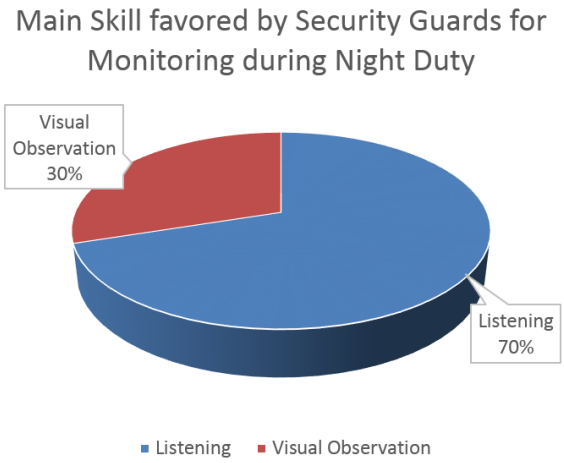

Fig. 17. Main Skill Favored by Guards for Monitoring in their Night Duty

3.2.12 Security Guard Preferences on Introduction of Mobile Application Solution. To find out the favor the proposed mobile application had among security guards in order to study their level of readiness in adopting it, a question was asked to a total of 20 of them on whether they would favor its entrance to the market. Before doing this, there was a keen explanation for them on the proposed application's advantages and key functionalities. 13 of the guards favored its introduction, citing effectiveness and efficiency as their main reasons. The remaining 7 were afraid and thus rejected its introduction, with their main fear of losing jobs.

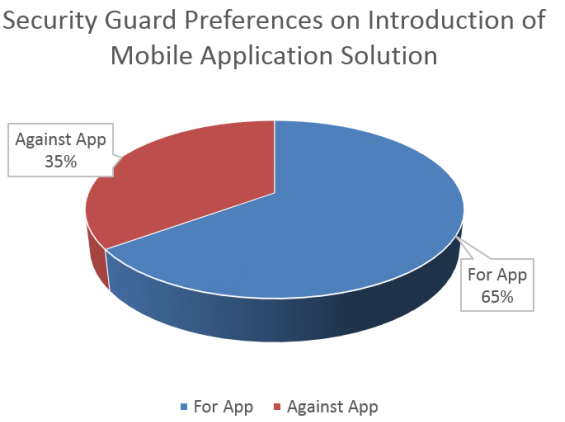

Fig. 18. Security Guard Preferences on Introduction of Mobile Application Solution

3.3 System Architecture

The following represents a system architecture of the system:

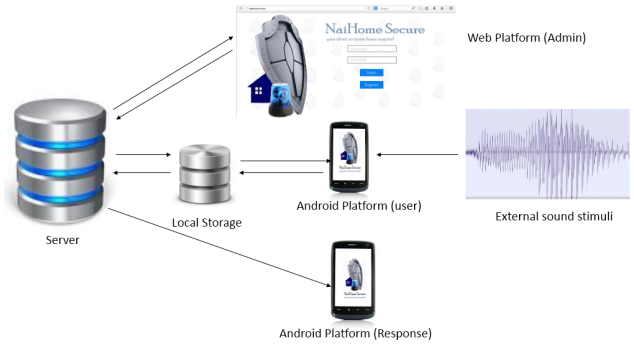

Fig. 19. System Architecture

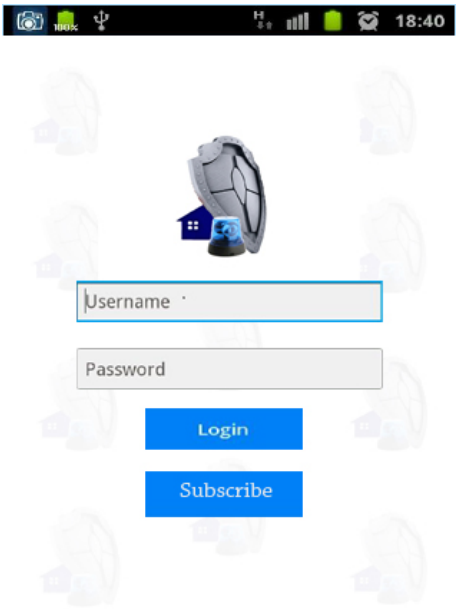

Fig. 21. Application Login Screen

3.4 Implementation Diagrams

The following are a sequence of important implemented application and admin end systems.

Fig. 20. Application Splash Screen

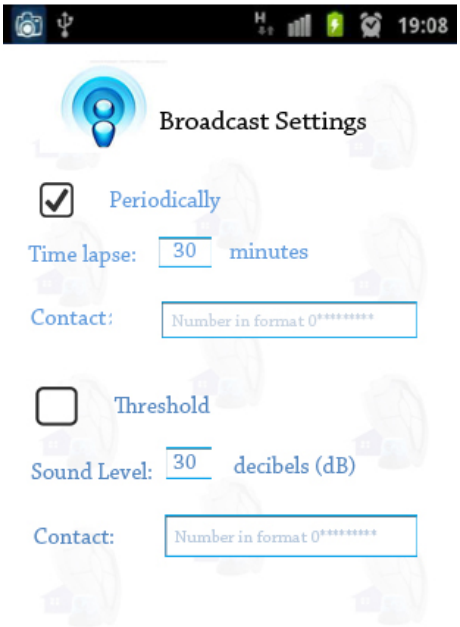

Fig. 22. Application Broadcast Setting

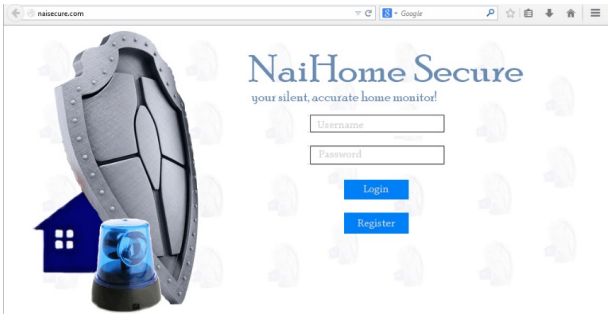

Fig. 23. Admin End Login

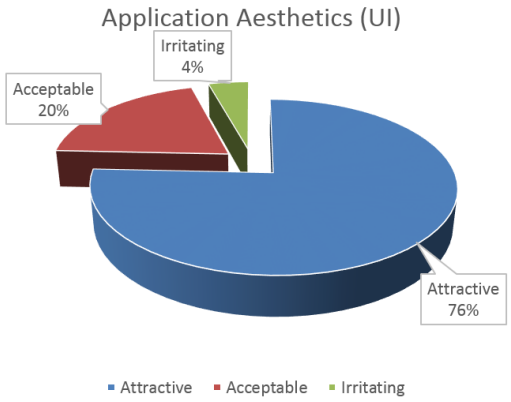

Fig. 24. App Aesthetics/UI User Testing

3.5 System Testing

This section details the various tests performed on the application and puts down the results using charts alongside detailed explanations.

3.5.1 Testing Environment. The application testing was carried out by a total of 70 users living and working around Nairobi County. Most of the users that tested the application were also involved in the initial stage of information collection. The developer of the application also had a share of testing to do before distributing the application for external testing.

3.5.2 Developer Functional and Compatibility Testing. The representation of this will be done by using tables. The tables will have the following content type: module name, description of test carried out, expected behaviors, observed behavior, and a comment. The tests were done on both user and administrative sides.

3.5.3 User Side: Functional Requirement Testing. The functional testing were orchestrated to see how satisfactorily the application and the web administrative end fulfilled the set functional requirements by both the developer and the interviewees.

3.5.4 Compatibility Testing. This test was done to ensure that maximum number of devices were compatible with the developed proposal. Both Android platforms on the user application end and the browsers on the administrative end were tested.

3.5.5 User Testing. User testing is an important process in the testing regime too given that the end users of the application are directly involved in having a hands-on experience of the application. This section of testing will involve various aspects that the users will be involved in: aesthetics, user friendliness, functionality, and acceptability. All these aspects will be given in forms of various calculations and chart to ensure a clear perspective of each element is viewed.

3.5.6 User Interface/Aesthetic Value. An information gathering on the application's aesthetic value based on its User Interface was carried out and the results were obtained from a total of 70 correspondents. Given options between Attractive, Average, and Irritating, 53 of the correspondents selected Attractive, 14 responded Average, while only 3 gave the negative feedback of Irritating.

3.5.7 User Friendliness. On user friendliness, the few menus and clear outline of the application were both great influencers in ensuring that over 80 percent of the testers were able to attest to the application's user friendliness. Given the options of Easy, Average, and Difficult, 56 users selected Easy, as 9 chose Average. Only 5 chose Difficult.

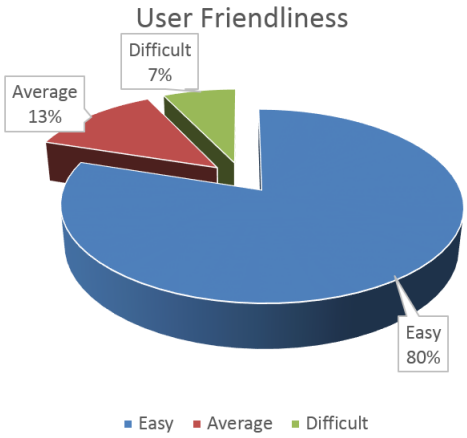

Fig. 25. App's User Friendliness Testing

3.5.8 Functionality. Functionality was the most important feat in the entirety of the project's scope. This is because a solution was supposed to be brought up that satisfied both the user requirements and the developer's requirements. To measure how the application did this, the users were asked to mention the functionality satisfaction level while using the application using a rubric of 10-25% meaning poor, 26-50% meaning just below average, 51-75% to mean fair, and 76-100% to mean good. Of the 70 respondents used for testing the application, 52 categorized the app as good, 18 categorized the application as fair, and 4 categorized the application as just below average.

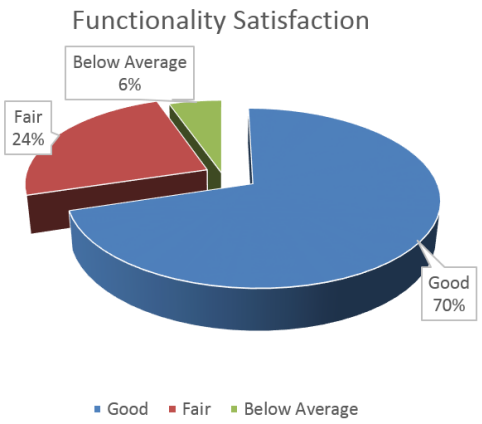

Fig. 26. App's Functionality User Satisfaction Testing

3.5.9 Acceptability. This study was carried out among the testers to determine how acceptable the population would be with the application, and how quickly they would adopt it. Of the 70 testers, 59 said they would readily accept the application, 8 were not sure, while 3 rejected the application and favored other security options.

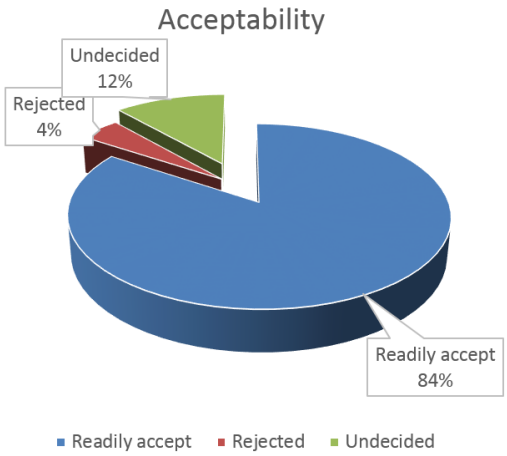

Fig. 27. App's User Acceptability Test Results

4. CONCLUSIONS, RECOMMENDATIONS AND FUTURE WORKS

4.1 Conclusions

In the wake of many insecurity threats in the country, coming up with an accurate and reliable security monitoring solution has been one of the greatest challenges. The constraints in coming up with solutions that include expense, portability, accessibility and reliability have pushed the challenge a notch higher. However, the advent of mobile technology and its rate of growth have indicated a lot of hope in coming up with a reliable application that would ensure real-time security monitoring and feedback relaying. This paper has documented the successful project scope that led to a mobile application able to harness the power of Natural Language Processing (NLP) in voice and sound recognition, message broadcasting and GPS services for monitoring and alerting purposes, optimized for a home environment during the night.

The application created harnessed the voice to trigger the disbursement of alert messages with regard to the preference of the user of either sending the alerts periodically or when a certain threshold is reached. This innovation is aimed at the facilitation of a trigger system that will be of applicability in situations where the household users cannot access their phone devices. The impulse reaction by humans in drastic situations to produce high-pitched voices was the main motivation of this study. The application will also help eliminate the need of physically station security personnel within premises, limiting their presence only when necessary after an alert has been broadcasted.

Despite this technological milestone in security agency monitoring, there is still more room to innovate and implement even better technologies. Artificial intelligence, a field that has of late come up strongly, has tended to be the motivation behind many mobile innovations. The field of mobile voice and sound technology is bound to go beyond the horizon and the limits that currently exists, broadening the opportunity to create more effective and efficient mobile applications.

The challenges faced in the scope of this research could be overcome to expand the target population for requirement analysis, testing and implementation in order to justify its viability and application. Financial and time constraints that also setback the scope of the research by limiting it to only manageable locations and implementations could also be eliminated to ensure a better technological approach to include most other artificial intelligence implementations in order to optimize the application.

4.2 Recommendations and Future Works

Despite the novelty of this study in the security field in developing countries, much more is left to be desired given the extent that technology scales in the contemporary world. Daily, innovative mobile technologies are emerging, and there is further room for development especially in the area of study in this scenario. Some of the suggested research that could be furthered in the scenario with regard to security monitoring with the aid of sound include:

—Research on how the application can detect, isolate and dispel any noise made by selected individuals to avoid any false positives.

—Implementation of an intelligent way to plot and detect noise in real time on a digital map.

—The implementation of a technique to detect various emotions within the environment that would precisely identify the scenarios in context to increase accuracy in monitoring and alerting.

—Application of a similar technique as proposed in this work in diverse equipment with the capability to listen to the environment apart from just mobile devices that would increase the scope of application.

The immediate research follow-up is a look at various emotions that the human voice contains in a bid to be able to isolate specific emotions that will further help in the automatic detection of criminal incidences with regard to security.

5. REFERENCES

[1] Armorvox. Voice versus speech: Voice biometrics compared to speech recognition, 2013.

[2] Jiangfan Feng and Yanhong Liu. Wifi-based indoor navigation with mobile gis and speech recognition. *Int. J. of Computer Science*, 9(6), 2012.

[3] Rob Huddleston. *Android Fully Loaded*. John Wiley & Sons, 2012.

[4] Commonwealth Human Rights Initiative. The kenya police service - commonwealth human rights initiative, 2013.

[5] Anish Joshi. Active web alert service for rule based alerting in sensor web an event based approach. *International Institute for Geo-information Science and Earth Observation MS Thesis*, 2005.

[6] Moses Kemibaro. The rise of low-cost android smartphones in kenya could mean the end for blackberry and nokia., 2012.

[7] Wichuda Kowtanapanich, Yordphol Tanaboriboon, and Witaya Chadbunchachai. An integration of hand-held computers, gps devices, and gis to improve the effeciency of ems data system. *Journal of the Eastern Asia Society for Transportation Studie*.

[8] Petros Maragos, Alex Potamianos, and Patrick Gros. *Multimodal processing and interaction: audio, video, text*, volume 33. Springer Science & Business Media, 2008.

[9] Michael J McGrath and Cliodhna Ní Scanaill. *Sensor Technologies: Healthcare, Wellness and Environmental Applications*. Apress, 2013.

[10] Kennedy Mkutu. The private security industry in kenya: Issues and challenges. In *Private Military and Security Companies*, pages 177–201. Springer, 2007.

[11] Mobithinking. Global mobile statistics 2013 part a: Mobile subscribers; handset market share; mobile operators., 2013.

[12] Manuel Mora. *Research methodologies, innovations and philosophies in software systems engineering and information systems*. IGI Global, 2012.

[13] MozquitoBytes. Be quiet - the noise alert., 2013.

[14] Mithun Kumar Ranganath. *Safety notification broadcast system*. PhD thesis, San Diego State University, 2012.

[15] Philip Tresadern, Chris McCool, Norman Poh, Pavel Matejka, Abdenour Hadid, Christophe Levy, TF Cootes, and Sebastien Marcel. Mobile biometrics (mobio): Joint face and voice verification for a mobile platform. *IEEE pervasive computing*, 99, 2012.