



2016

A Mobile and web based application for security intelligence gathering: a case study of Nairobi County

Francis Omolo O.
@iLabAfrica
Strathmore University



Follow this and additional works at: <https://su-plus.strathmore.edu/handle/11071/4864>

Recommended Citation

Omolo, F. O. (2016). *A Mobile and web based application for security intelligence gathering - a case study of Nairobi County* (Thesis). Strathmore University. Retrieved from <http://su-plus.strathmore.edu/handle/11071/4864>

**A MOBILE AND WEB BASED APPLICATION FOR SECURITY INTELLIGENCE
GATHERING: A CASE STUDY OF NAIROBI COUNTY**

OMOLO FRANCIS OMONDI

**Submitted in partial fulfilment of the requirements for the Degree of Masters of Science in
Mobile Telecommunications and Innovation at Strathmore University**



**Faculty of Information
Strathmore University**

Nairobi, Kenya

June, 2016

This dissertation is available for Library use on the understanding that it is copyright material and that no quotation from the dissertation may be published without proper acknowledgement.

Declaration

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the dissertation contains no material previously published or written by another person except where due reference is made in the dissertation itself.

© No part of this dissertation may be reproduced without the permission of the author and Strathmore University.

Name: Omolo Francis Omondi

Signature:

Date:

Approval

This dissertation of Omolo Francis Omondi was reviewed and approved by the following:

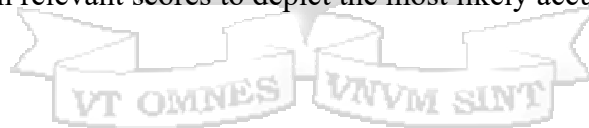
Dr. Vitalis Ozianyi,
Senior Lecturer, Faculty of Information Technology,
Strathmore University

Dr. Joseph Orero,
Dean, Faculty of Information Technology,
Strathmore University

Prof, Ruth Kiraka,
Dean, School of Graduate Studies,
Strathmore University.

Abstract

The security situation in Kenya has deteriorated over time due to the low number of police personnel in the country which is currently at a population ratio of 1:1150. Security challenges have increased from mere theft to carjacking attacks and to more serious and evolved challenges like murder and terrorism. The government's efforts towards reducing these crimes have been ineffective as there are no mechanisms for gathering intelligence at low levels. Intelligence gathering especially from the public is very essential in tackling matters to do with insecurity. This research proposes a simple, convenient and efficient solution to the security challenges that Kenya is currently facing with respect to systematic gathering of intelligence and its analysis by the use of a mobile and web based application. The mobile based solution will integrate the use of GPS location services and ensure that it uses machine learning by using predictive models produced from Multiclass Decision Forest Algorithm, and to be able to provide detailed descriptive statistical analysis, text mining analysis of criminal activity taking place, as well as prediction analysis to predict crime patterns. The solution has an administrative web-based backend that will be accessed by the police force to ensure they get detailed information of criminal activities. From this portal, tests were done by entering information regarding suspicious person, potential suspicious person names associated with the submitted information are provided together with relevant scores to depict the most likely accurate name.



Dedication

I dedicate my dissertation work to my family and friends whose words of encouragement and support during this period.



Acknowledgements

This research project would not have been possible if it were not for the support and the dedication of a number of people first and foremost I would like to thank God for the blessings and inspiration throughout the project. I must also thank my supervisor Dr Vitalis Ozianyi for their supervision. I would also like to thank Strathmore University for providing a suitable environment for the completion of my report.

Special thanks to my family for providing the encouragement. Also I would like to thank my colleagues and friends, not forgetting all those who took interest in an attempt to get any information that was relevant to the progress of this project.

Finally, Thank you to those whom I have not mentioned but assisted in this project in one way or the other and those who supported me in my efforts.

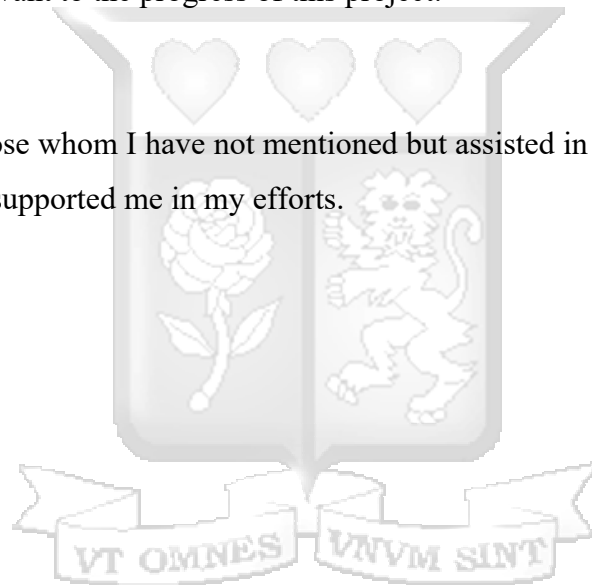


Table of Contents

| | |
|---|-----|
| Declaration..... | i |
| Abstract..... | ii |
| Dedication..... | iii |
| Acknowledgements..... | iv |
| List of Figures..... | x |
| List of Tables..... | xi |
| Abbreviations/Acronyms..... | xii |
| Chapter 1 : Introduction..... | 1 |
| 1.1 Background of the Study..... | 1 |
| 1.2 Problem Statement..... | 2 |
| 1.3 Research Objectives..... | 2 |
| 1.4 Research Questions..... | 3 |
| 1.5 Justification..... | 3 |
| 1.6 Scope..... | 3 |
| 1.7 Limitations..... | 4 |
| 1.8 Ethics in Research..... | 4 |
| Chapter 2 : Literature Review..... | 5 |
| 2.1 The State of Security in Kenya..... | 5 |
| 2.1.1 The Security State..... | 5 |
| 2.1.2 Current Responses to the Security State..... | 6 |
| 2.2 New Technologies for Tackling Security Challenges in Kenya..... | 7 |
| 2.2.1 Tackling Security Challenges Using Technology..... | 7 |
| 2.2.2 Kenyan Police Engagement with Technology: Social Media and SMS..... | 8 |
| 2.3 The Use of Tackling Security Challenges..... | 9 |

| | | |
|---------------------------------------|---|----|
| 2.3.1 | Mobile Phones Penetration | 9 |
| 2.4 | Use of Mobile Applications in Crime Reporting | 10 |
| 2.5 | Crime Information Collected by Police Application..... | 11 |
| 2.6 | Automating Crime Reporting Using Mobile Phones and Computers..... | 12 |
| 2.7 | Mobile Application Architectures | 15 |
| 2.7.1 | Thin Clients..... | 16 |
| 2.7.2 | Fat Clients | 16 |
| 2.7.3 | Server Architectures: Three-Tier Server architecture..... | 16 |
| 2.7.4 | Connection Synchronization..... | 18 |
| 2.7.5 | Information Security | 18 |
| 2.7.6 | Crime Analysis and Mapping | 20 |
| 2.8 | Machine Learning and Artificial Intelligence | 23 |
| 2.9 | Text Mining and Analytics..... | 23 |
| 2.9.1 | R and Azure Machine Learning Platforms | 23 |
| 2.9.2 | Use of both R and Azure Machine Learning for Text Mining | 23 |
| 2.9.3 | Packages in Text Mining | 23 |
| 2.9.4 | Term Document Matrix and Document Term Matrix | 25 |
| 2.10 | Synthesis and Gaps in Literature Review | 26 |
| Chapter 3 : Research Methodology..... | | 27 |
| 3.1 | Research Design..... | 27 |
| 3.2 | Location of Study | 27 |
| 3.3 | Data Collection..... | 28 |
| 3.3.1 | Mobile Application Input..... | 28 |
| 3.3.2 | Document Reviews | 28 |
| 3.4 | Data Analysis | 29 |

| | | |
|---|---|----|
| 3.5 | Validity and Reliability | 29 |
| 3.6 | Quality of the Research Instruments | 31 |
| 3.6.1 | Efficiency | 31 |
| 3.6.2 | Reliability..... | 32 |
| Chapter 4 : System Design and Analysis..... | | 33 |
| 4.1 | System Design..... | 33 |
| System Architecture | | 33 |
| 4.1.1 | Client Side..... | 34 |
| 4.1.2 | Server Side..... | 34 |
| 4.2 | Data and Process Modelling..... | 35 |
| 4.2.1 | DFD Models..... | 35 |
| 4.2.2 | Use Case Modelling..... | 36 |
| 4.3 | Database Design` | 37 |
| 4.3.1 | The Relational Database Schema..... | 37 |
| 4.3.2 | The NoSQL Database Schema..... | 39 |
| 4.4 | Security Design | 40 |
| 4.4.1 | Analytics and Machine Learning..... | 40 |
| 4.5 | Text Mining and Analytics..... | 40 |
| 4.5.1 | Introduction to Text Mining..... | 40 |
| 4.5.2 | Reading the Data..... | 40 |
| 4.5.3 | Pre-processing of the Read Data..... | 41 |
| 4.5.4 | Sourcing data into the R platform..... | 41 |
| 4.5.5 | Data Pre-processing | 42 |
| 4.5.6 | Term Document Matrix and Frequent Terms | 44 |
| 4.6 | Machine Learning and Prediction | 44 |

| | | |
|--|--|----|
| 4.6.1 | The Raw Dataset | 44 |
| 4.6.2 | The Split Datasets | 46 |
| 4.7 | Results and Findings | 50 |
| 4.7.1 | Distribution of Locations | 50 |
| 4.7.2 | Distribution of Persons | 53 |
| 4.7.3 | Distribution of Organisations..... | 56 |
| 4.7.4 | Distribution of Websites and URLs..... | 59 |
| 4.7.5 | Distribution of Keywords | 61 |
| 4.8 | Development | 64 |
| 4.8.1 | The Mobile Application..... | 64 |
| 4.8.2 | The Web Application..... | 64 |
| 4.8.3 | The Pre-Processing APIs | 64 |
| 4.8.4 | The Machine Learning System..... | 64 |
| Chapter 5 : System Implementation and Testing..... | | 65 |
| 5.1 | Introduction | 65 |
| 5.2 | Client Side System..... | 65 |
| 5.2.1 | Android Versions Support | 65 |
| 5.2.2 | Android Libraries..... | 65 |
| 5.2.3 | Mobile Application Communication Endpoints | 66 |
| 5.2.4 | Input Validations..... | 67 |
| 5.2.5 | Application Components | 67 |
| 5.3 | Web Services and Middleware..... | 71 |
| 5.3.1 | Integration with mobile application..... | 71 |
| 5.3.2 | Integration with third party analytics APIs..... | 71 |
| 5.3.3 | Integration with database management infrastructure..... | 71 |

| | | |
|------------|---|----|
| 5.4 | Server Side Web Administration Application..... | 72 |
| 5.4.1 | Web Application Environment | 72 |
| 5.4.2 | Application components | 74 |
| 5.4.3 | Application security | 75 |
| 5.5 | System Testing | 75 |
| 5.5.1 | Mobile application testing..... | 75 |
| 5.5.2 | Web application testing..... | 77 |
| Chapter 6 | : Discussions of Results from the Testing..... | 79 |
| 6.1 | Review of Research Objectives in Relation to the Mobile Application | 79 |
| 6.2 | Review of the Proposed System..... | 80 |
| 6.2.1 | Advantages of the Proposed System..... | 80 |
| 6.2.2 | Limitations of the Proposed System | 80 |
| 6.3 | Summary | 81 |
| Chapter 7 | : Conclusions and Recommendations | 82 |
| 7.1 | Conclusions | 82 |
| 7.2 | Recommendations..... | 82 |
| 7.3 | Future Work | 83 |
| References | | 84 |

List of Figures

| | |
|---|----|
| Figure 2-1: Crime reporting information upload (Agangiba & Akotam, 2013)..... | 12 |
| Figure 2-2: Three-tier server architecture (Lee, Schneider, & Schell, 2010) | 17 |
| Figure 2-3: Two-tier server architecture (Lee, Schneider, & Schell, 2010) | 17 |
| Figure 2-4: Store and Forward Synchronization (Lee, Schneider, & Schell, 2010)..... | 18 |
| Figure 2-5: RSA Cryptosystem (Ogwueleka & Ocheme, 2014) | 19 |
| Figure 2-6: Crime Analysis Process (Crime Analysis Defined, 2005)..... | 21 |
| Figure 2-7:2014 UCR Part I Crime (Source: ARJIS)..... | 21 |



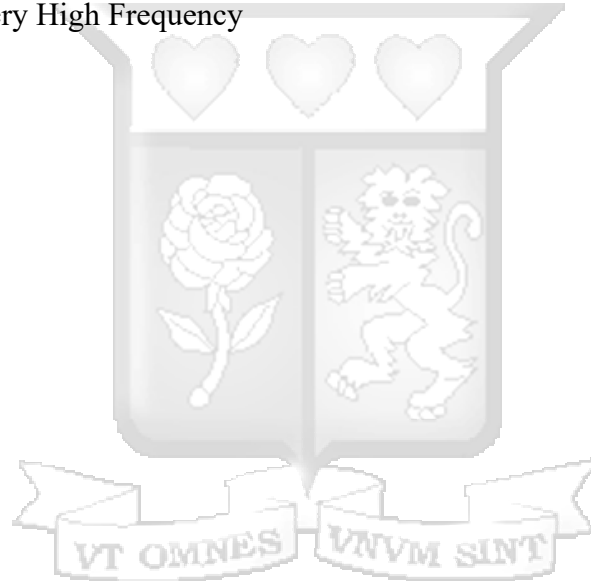
List of Tables

| | |
|--|----|
| Table 2-1: Crime Reporting Mobile Application..... | 15 |
| Figure 3-1: Machine Learning Life Cycle | 31 |
| Table 5-1: Suspicious Person Submit Test Case..... | 76 |
| Table 5-2: IP Restricted Authentication Test Case..... | 77 |



Abbreviations/Acronyms

| | | |
|---------------|---|--|
| API | - | Application Programing Interface |
| CDN | - | Content Delivery Network |
| CRECO | - | Constitution and Reform Education Consortium |
| GPS | - | Global Positioning System |
| SaaS | - | System as a Service |
| SODNET | - | Social Development Network |
| VHF | - | Very High Frequency |



Chapter 1 : Introduction

1.1 Background of the Study

Unlawful activities, in Kenya, have been a rising concern for the Kenyan citizen and the security personnel. The way of life of most residents in Kenya has been hindered while security officers have been undermined in sufficiently managing the rising crime rates. The inadequacy of the police authority to maintain the security and wellbeing concerns of the Kenyan residents could be attributed to the few numbers of the police. This has been worsened by the fact that some police officials are bribed by criminal offenders, leaving the rest of the police to manage crimes that rise within Kenya. The police ratio left is at a ratio of 1:1150, which means 1 police official to manage crimes within a population of 1150 which is far beneath the UN-proposed ration of 1:450 (Commonwealth Human Rights Initiative, 2013).

Most people decide to source for security from private institutions such as Absolute Security Ltd. Access systems, G4S security services Kenya and others. However not everyone can afford the fees that private institutions charge and thus face the risk of being attacked by criminals. Criminal offenders exploit the unequipped state of the citizens to discover methods of avoiding detection when they carry out their criminal activities. In spite of this, numerous companies still emphasize on their need of offering security services at a high cost given the urgency on the need for security.

This dissertation aims at documenting a mobile and cloud application for intelligence gathering system that will ease the insecurity in Nairobi. The researcher proposes a simple, convenient and efficient solution to the security challenges that Kenya is currently facing geared towards systematic intelligence gathering and analysis by the use of a mobile and cloud application. The application takes advantage of this upcoming technology to allow users to feed information about suspicious activity within their surrounding and post it to a central database that will be hosted at the Kenya Police headquarters. The crowd sourced information will be carefully analysed using special analytics algorithms and useful patterns and clues established for the authorities to take more accurate action in an effort to curbing insecurity in Kenya.

1.2 Problem Statement

There has been constrained usage of cell phone innovations for the execution of security alert solutions which cater to the Kenyan population, requiring the need of physically deploying security personnel in the event of any criminal activities. The use of a cloud based solution, has been underutilized given the flexibility and ability that Android devices have in accommodating cloud solutions. This has made existing security solutions to lack having a special analytics algorithms patterns that will offer clues on existing crime and potential areas where crime is likely to occur. Most existing applications utilize GPS but are only activated strictly when a user prompts the application. This practicability would not be useful in gathering vital information that could be used to compare criminal pattern activities that would help police officers investigate crime efficiently. In such situations, there emerges a need to execute an application that will consequently provide a portal where information regarding criminal actives is stored and analysed in order to detect a pattern in criminal activity and be able to draw conclusions that would assist in preventing further crime from taking place.

Data on criminal activities are not effectively stored thus making it difficult to fight crime in Kenya. The integration of a cloud based mobile application to the android platform, would let citizens report criminal activities that are taking place and would provide the police personnel with relevant information which they can use to come up with preventive measures against crime.

1.3 Research Objectives

The research objectives are:

- i. To identify the current advancements in technology used to capture informational regarding criminal activities.
- ii. To determine the challenges experienced by the population in terms of reporting crime and analysing criminal activities.
- iii. To design and develop a mobile application that can let users report crime and enable authorities draw analytical conclusion that can prevent the same crime for occurring again.

- iv. To perform the required system testing on the mobile application.

1.4 Research Questions

- i. What are the advancements in technology used to capture information regarding criminal activities?
- ii. What are the challenges experienced by the population in terms of reporting crime and analysing criminal activities?
- iii. How will the application be designed and developed?
- iv. How will the application's functionalities and goals be tested?

1.5 Justification

Crime in Kenya is growing at an alarming rate and there is a significant amount of data collected by the police but it is poorly stored hence inaccessible to draw up analytical conclusions when needed. In some situations the police take priority in trying to solve the crime rather than try store the data to prevent a similar crime taking place. Moreover, the information collected is not comprehensive enough to draw up conclusions on criminal activities taking place. This leads to criminal offenders evading justice and similar crimes taking place over and over.

The research will illustrate the importance of customary analysis on criminal activities to establish a pattern which can be used to capture criminals and prevent crimes from taking place. The results will be accessible to the authorities and will help them in investigating crime. The public will also be able to report any criminal or suspicious activities that they witness, which will be stored and used by the authorities.

1.6 Scope

The main focus of the study is to develop a mobile based cloud solution that uses artificial intelligence to analyse and store collected data. The data will be collected through the use of a mobile application and the analysis of the results will be done on a web interface. The application will use artificial intelligence to implement an algorithm that will group relevant criminal data in an efficient way that will generate information that will assist authorities in their day to day activities.

1.7 Limitations

The following are limitations that the researcher will encounter during the research process:

- i. Police may not easily be willing to provide information due to confidentiality issues.
- ii. The population may not be willing to respond with truthful answers regarding criminal activities occurring in their area due to fear.
- iii. Getting information may prove to be a challenge as most of targeted people may not be willing to use mobile applications.

1.8 Ethics in Research

Ethics is essential in completing research as it guarantees that moral rules are placed when communicating with members who will be included in the study. The moral issues that will be connected in the study include the following:

- i. Consent: This includes the system by which research subjects will be selected.
- ii. Privacy: This will include guaranteeing that any classified data the researcher is given will not be misused.
- iii. Honesty: Ensuring that the study is not copied from any previous research done.



Chapter 2 : Literature Review

In the recent past, Kenya, like most African countries, has experienced high levels of crime and violence and a minimally low safety index of 21.01. This ranges from acts of basic criminality to social and systemic violence with the potential to destabilize social cohesion and state functionality. Several explanations have been advanced for the upsurge, ranging from issues of the high levels of unemployment, the proliferation of small arms and light weapons from the porous borders that are used for cattle rustling and armed robberies. In this literature review, we present the current state of security in Kenya and especially Nairobi County and measures that have been taken to respond to this state. The review then exposes the ways in which a mobile application can be used to securely and anonymously collect security tips from users. Using this motivation, a mobile application will then be proposed to utilize the capabilities of a smart phone, which will be used to address the raised issues.

2.1 The State of Security in Kenya

2.1.1 The Security State

Kenya, like most of sub-Saharan Africa has in the recent past experienced exponentially high levels of crime and violence with a crime index rate of 78.91 and a minimally low safety index of 21.01 (Omondi, 2013). The insecurity experienced in Kenya especially in Nairobi results from activities of Kenyan citizens and those from terrorists. In the recent past, Kenya has been a target to terrorism. Kenya was not simply chosen at random by terrorists. Quite the opposite, there are several factors that contribute to making Kenya an attractive target. These, in turn, make Kenya a priority for the Global War on Terror. These factors include geography, ethnic composition, political stability, unstable neighbours, poverty, Islamic fundamentalism, and lax law enforcement. Internally, several explanations have given to elaborate the causes of insecurity in Kenya including issues of the high levels of unemployment, the proliferation of small arms and light weapons from the porous borders that are used for cattle rustling and armed robberies, the intra and inter-state conflicts, the fight for trans-boundary resources, to the drought and famine experienced in various parts of Kenya (Aronson, 2013).

Crimes also result from informal settlement living conditions. For example, like other informal settlements in Nairobi, Kibera and Mathare slums are characterized by high population density, unplanned and crowded housing, and lack of basic infrastructure. Most roads are inaccessible to

vehicles, drainage channels are often blocked, and heaps of uncollected garbage are scattered everywhere. In addition, insecurity is a big problem, and has forced residents to resort to the informal security offered by gangs (Mutahi, 2011). This cycle makes security a complex undertaking. This is also so because the majority of poor people in urban slums live on the margins of ‘illegality’, which is characterised by unlawful acquisition of housing, non-payment of taxes, and the illegal tapping of water and electricity, among others. The government has been unable to adequately provide these services to slum residents, who are consequently forced to rely on gangs for service provision, at a fee (Mutahi, 2011).

2.1.2 Current Responses to the Security State

The Kenyan constitution identifies the police as the officers who maintain law and order. They are also supposed to keep internal security. The Kenyan army, navy and air force keep Kenya’s external security for water ways, air and land respectively. All these groups depend on the intelligence from the Kenya’s intelligence service. However, the police citizen ration is very small: 551 by 2012. This is against the United Nations’ optimal ratio of 1:400 (Herbling, 2012). Often, police encourage the public to report crimes. Currently, there are toll free numbers, which have been set up to let the public report crimes. However, the public do not prefer them because the call centres have to find more about the incident from the caller. Besides, there are not enough staff to respond to the calls. The public can also report crimes directly to the police. However, a report by a state agency indicates that members of the public still fear to report to the police when crime occurs. This is because police officers are ‘the enemy’ to the public (Otiono, 2013). Paramount is that the public who may report crimes fear for their own lives as they may not be protected if they will be witnesses (Herbling, 2012). Depending on these means would not help collect the necessary intelligence that would lead to reaching the perpetrators. Also, the intelligence gathered this way is not timely.

In 2003, the government launched an initiative to bring communities and police together through community policing. The purpose was to involve communities in defining and setting an agenda for dealing with crime and violence based on the realities of the local context (Omondi, 2013). According to Kenya Police, community policing is the perceived effort to enhance security thus recognizing the interdependence and shared responsibility of the police and the community in ensuring a safe and secure environment (Omondi, 2013). Furthermore, an active partnership

between the police and the public to combat crime and enhance community safety is the core theme of Kenya's community policing. Community policing works by creating an understanding between the police and the community about their role in crime prevention.

Community policing was started but has a number of challenges. For example, there is a problem of manpower management owing to the poor police to citizen ratio. Corruption, among police officers, existence of mistrust and inadequate sensitization of community policing to the community members are other challenges of community policing.

In the year 2014, the governments of Kenya introduced the Nyumba Kumi initiative to enable the public take part in ensuring their security. The government thought that that Kenyans' participation was the surest way to help realise their mandate as per the Constitution (Kariuki, 2014). The era of leaving everything to the government is long gone and Kenyans must know that they also count. However, besides the problem of funds to initiate smooth operations of the Nyumba Kumi initiative, Nairobi residents are less concerned with the neighbours because they are strictly in pursuit for opportunities while majority enjoys their sweat in pubs and restaurants (Adika, 2014).

2.2 New Technologies for Tackling Security Challenges in Kenya

2.2.1 Tackling Security Challenges Using Technology

Over the last few years, Kenya, especially Nairobi, has experienced rapid advancement in the use of mobile technology and is today considered a leading hub for ICT innovation in Africa. Open source software such as Ushahidi (a crowd sourcing online mapping system set up in days to document incidents of violence following the 2007 national election) has put Nairobi on the global map as a place where tech savvy youth from across Kenya, and around the world, come together to develop innovative solutions to a wide range of social, economic and security challenges (Frilander *et al.*, 2014).

Ushahidi helped citizens tell their story through SMS and social media, relating that information back to the geographic location where the story or incident took place. The software as well as the organization with the same name has grown quickly and the tool is used for various purposes by organizations all around the world (Frilander *et al.*, 2014). In 2010 and 2013, Ushahidi partnered with Hivos International, SODNET, CRECO and other organizations to deploy two projects related to Kenyan votes. The first project monitored the Kenyan Referendum of 2010

and the second project, the 2013 general elections. Uchaguzi Kenya 2013 was a short-term deployment of the crisis-mapping platform to act as an early warning and response system during the election.

Another example of initiatives to use ICTs to improve public security is *Sisi Ni Amani – Kenya*'s, use of SMS and mobile technology for communication and violence interruption. While such a tool could potentially help police keep law and order through faster incidence response and smarter police patrolling patterns, the police do not appear to have used this technology systematically, except perhaps around the general election in March 2013 (Frilander *et al.*, 2014).

2.2.2 Kenyan Police Engagement with Technology: Social Media and SMS

There is comparatively limited formal engagement with ICTs among large segments of the National Police Service. Interviews with police officers in several of Nairobi's informal settlements and at the city's central police station revealed that the incorporation of new technologies is limited and sporadic. This finding is consistent with the assessment of Kenyan academics and practitioners interviewed during this research. Street level patrols are not issued with mobile phones or airtime for work. Some officers are issued with a VHF radio, although they are frequently in poor condition and seldom used (Frilander *et al.*, 2014). A minority of younger police officers also appear to have smartphones and use them for accessing social media for entertainment and socialising with friends. Only one of the police officers interviewed mentioned the use of Google maps to identify locations and routes for work purposes. Of the senior police officers interviewed many of them own high-end smart phones but do not necessarily use them for work purposes in a systematic manner (Frilander *et al.*, 2014).

However, there are examples of innovative use of ICTs by individual security providers. Chief Francis Kariuki, the administrative chief of Lanet Umoja in Western Kenya, is using Twitter (@Chiefkariuki) for collaborating with the public in order to reduce crime in his location. He has more than 29,600 followers on Twitter and it is reported that by communicating with his constituents about everything from the disappearances of animals to household burglaries (Sitole, 2012). Using 140 characters or less, Chief Francis Kariuki in Kenya, has tweeted his way to

reducing crime in his and surrounding villages. Kariuki sends messages to over 15,000 of the 28,000 people who live in Lanet Umoja (Omanga, 2015). They include village elders, community and church leaders, the police, youth and women's groups, and school principals (Sitole, 2012).

According to a survey carried out by Frilander *et al.*, in the year 2014, it showed that the police agreed to the following advantages of adapting new technologies:

- Enhance communication and coordination between officers on patrol and with superior officers in the police stations without fear of their information being diverted or misused,
- Identify locations and routes more easily and identify the best and/or closest resource to an incident,
- Enable police officers patrolling in dangerous areas to more easily request and get reinforcement,
- Introduce digital records, which would be more efficient than the current “pen and paper” system, especially if police files could be accessed remotely by officers on patrol.

2.3 The Use of Tackling Security Challenges

2.3.1 Mobile Phones Penetration

According to a survey carried out by Frilander *et al.*, in the year 2014, mobile phone ownership among the police and wider slum population is virtually universal and there is stable network coverage throughout the city. Mobile phones are increasingly Internet-enabled (more than half of the surveyed population reported having this function). Smartphone ownership is not yet common in low-income neighbourhoods and among the lower-ranking officers in the National Police Service but this is likely to change over the coming few years. According to human IPO, smartphone penetration is 67%. Smartphones made up 67 per cent of devices sold by leading Kenyan operator Safaricom in 2013, with 100,000 new devices being purchased every month (Udemans, 2014). This growth is attributed to a growing middle class that has increased the uptake of these types of phones (Udemans, 2014). HumanIPO reported earlier this year Android's mobile operating system (OS), found on numerous smartphones including Samsung's, had become the most popular mobile OS on the continent.

2.4 Use of Mobile Applications in Crime Reporting

Recent researchers have identified mobile handheld devices as a possible tool for effective crime detection and reporting. Technological advancements have led to the invention of extremely powerful mobile handheld devices and have brought about large and high speed data transfer capabilities through mobile communication networks.

Smartphone shipments worldwide reached 485 million in 2011, increased to about 655 million in 2012, and expected to rise over one billion smart phones by 2016 (Agangiba & Akotam, 2013).

Another key factor making mobile phone technology a viable medium for fighting crime is the advancement of cellular networks technologies. The introduction of 3G/4G cellular network technologies by most mobile network operators has improved the communication demands for mobile users (Agangiba & Akotam, 2013). With these two factors in place, development of dedicated mobile platforms for detecting and reporting criminal activities is a great possibility.

The advancement of computer technologies has led to more effective ways of detecting and fighting crime in society. Today, engineers and researchers have proposed and developed a number of computer based systems, especially for crime detection and reporting. Previously, police officers have used cruiser-mounted Toughbooks and other ruggedized PCs that provide access to critical 911 call details, suspect information, and allow in-car mobile reporting. The drawback is that officers need to be in the car to be able to perform their tasks. With phones and tablets, officers can use these devices outside the vehicle, in unmarked cars, on motorcycle, and so on – this provides true mobility at a greatly reduced cost (Sun, 2014).

According to Agangiba & Akotam (2014), the most useful mobile applications for reporting crimes, should allow both the public and the police to interact with the application. Further, Agangiba and Akotam suggest that tip-offs sent by the application must be securely sent to a central server, and can only be seen by the police. This is to prevent an incident whereby the criminal himself, through his handheld device becomes aware that, a tip-off has been sent about him to the police. Also, if a member of the general public sends a tip-off to the police, the sender's location information as well as his registration details is also recorded on the server for

such sender's movement to be monitored at least for twenty-four hours by the police (Agangiba & Akotam, 2013).

2.5 Crime Information Collected by Police Application

Agangiba & Akotam (2014) proposes two groups of people, who must interact with a crime reporting application, police and the public

According to their model, the type of information, which can be uploaded to the server include:

- Descriptions of people on police wanted list and their related crime information
- Description of missing items and their related information
- Information about latest arrests made by police

On the other hand, the information, which can be uploaded by public include:

- Found items information – information of the whereabouts of items reported to the police as missing. This information is meant only for the police.
- Tip-offs of people on the police wanted list – Information of the whereabouts of people who are on the police wanted list.
- Tip-offs of on-going crimes – Information of criminal activities which are currently taking place
- Time of reporting and location are automatically registered by the application. However, the user is allowed to send the tips anonymously, this is without entering any details and extracting request IP.

Details of the uploaded entities must be included too. For example, for criminals, the name, age group, facial looks, complexion, weapons in possession, crime involved, other crimes associated with in the past are given if they are known. However, reporter should have a chance to give more information if they wish. They details include:

- When and where the incident occurred
- Weapons the suspect(s) carried
- Where and when the suspect(s) was last seen
- Description of the suspect(s) (including gender, race, age, height, weight, hair colour/length, clothing, facial hair, tattoos/scars)

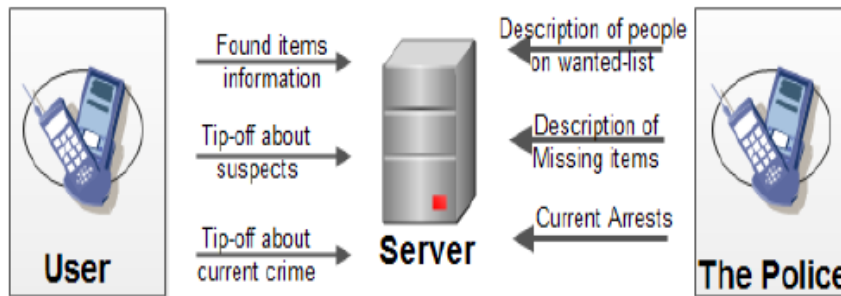


Figure 2-1: Crime reporting information upload (Agangiba & Akotam, 2013).

2.6 Automating Crime Reporting Using Mobile Phones and Computers

A number of engineers have successfully designed and developed application to automate crime reporting. This section presents an overview of some of the computer based crime fighting systems developed within the past six years. The overview pays attention to functionalities and principles of operations of these systems.

KaaRadah, is a Kenyan based solution for crime reporting. The name of the system is depicted from the Kenyan slang meaning, *be alert*. Users are prompted so sign up to the application, later which, they can report crimes anonymously. The user is provided a drop down menu containing the crime category that he/she wishes to submit, keys in the report, a popup dialog for more information appears, and finally he submits the data. However, the information that the users have submitted is not submitted for analysis, instead it is sent to other mobile users for alerting purposes. This however creates a risk for users to submit false information, and there is no way to validate if information is authentic. This information is not analysed to provide predictive features to curb potential threats before they happen.

Najua, is another Kenyan based system whose name is depicted from the Swahili word 'I know'. In this system, the users are able to submit crimes in their environment. Upon submission, this data is sent directly to police handsets in police stations. Should there be no action, the public are able to hold the police accountable for lack of prompt action in the event of an ongoing crime. In this system as well, no analysis is done neither filtering of spam to the police, nor misleading information nor false reports. This information is not analysed to provide predictive features to curb potential threats before they happen.

Crime Stoppers, New Orleans has launched a new free mobile crime-fighting application, for Android and iPhone platforms, called Tip Submit. The application was created by Tip Soft and Crime Reports and is known to be the first anonymous tip submission mobile software. By design, Tip Submit allows citizens to submit crime tips to Crime stoppers securely and anonymously. The system identifies tipsters by their tip number only, which it assigns to the tip (Agangiba & Akotam, 2013). The Mobile Application allows tipsters to upload photos or video and is able to send the location of the video by a GPS locator. Other key features of Tip Submit is that, it has no limits on the amount of text unlike with SMS text messages. Also, it maintains two-way dialogue and real-time chat between the tipster and Crime stoppers (Agangiba & Akotam, 2013). Crime stoppers is run by civilians, not law enforcement. Citizen tips remain anonymous, and those giving tips will never be asked to fill out a police report or testify in court. Crime stoppers works with law enforcement, but does not itself investigate crimes and does not prosecute criminals. Crime stoppers now accept tips on sex offenders, and gives up cash rewards to tipsters (nola.gov, 2014). Anonymous tips can also be submitted via an online application.

A system, called **Web-Cast** allows establish trends on the data, showing the types of crimes that commonly occur, and the places with which they are associated. By typing in specific dates, types of crimes, locations, and selecting names of weapons used, Web-Cat produces graphs, reports, and maps of high crime areas (Agangiba & Akotam, 2013).

Another computer based crime fighting tool is **Mobile Vic PD**. Mobile Vic PD is a recently released mobile application, released by the Victoria police in Canada for fighting crime. The mobile application can be used to report minor crimes, offer anonymous tips to police, stay updated on crimes in progress, receive missing child reports or check on stolen property (Agangiba & Akotam, 2013).

Accurint is produced by LexisNexis for the iPhone and iPad. This Mobile application connects government and law enforcement agencies to more than thirty billion public records and critical investigative tools needed to verify information in the field, and rapidly follow-up on new leads as they develop. The most widely used tactical lead generation tool for law enforcement in the

United States is cop link mobile plus app, created by i2. The application runs on iPhone, iPad and Android platforms (Agangiba & Akotam, 2013). The application enables officers to achieve better situational awareness with automated geospatial searches of recent events, as it allows the searching of state and local criminal records from multiple jurisdictions' databases. Another great feature of the application is its ability to organize vast quantities of seemingly unrelated data to assist in making tactical, strategic and command-level decisions (Jennifer, 2013).

The **PoliceOne.com** iPhone application is the best way for Police Officers and other Law Enforcement professionals to keep informed while on-duty or on the move. Stay up to date on breaking police news, videos, expert columnist articles, tactical tips and other relevant information. Whether you need to research something from your squad car or just want to browse the latest news, this application gives officers free access to mobile resources that have never been available to them before (PoliceOne.com, 2015). A version for Android and iOS are available. A summary of sample crime reporting mobile application is tabulated in Table 2.1 (Agangiba & Akotam, 2013).

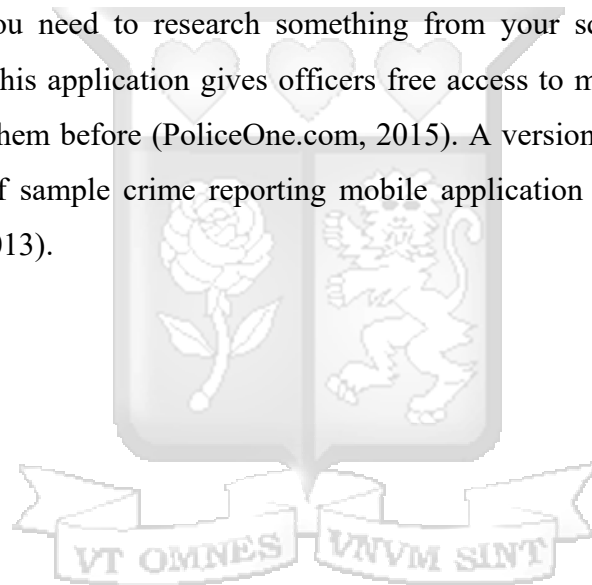


Table 2-1: Crime Reporting Mobile Application

| Application name | Advantage | OS/platform |
|------------------|---|-----------------|
| KaaRada | -Allows anonymous tips -Other application users get prompt danger alerts | Android |
| Najua | -Police get real time information regarding crimes | Android |
| Police One | -Has an option of submitting a tip anonymously. -Supports video media. | Android and iOS |
| Accurint | Verification of information in the field. | iOS |
| Mobile Vic PD | -Allows Anonymous tips -Allows updates of crime in progress | iOS |
| Webcast | -Associates crimes with places where they occur | Web-based |

2.7 Mobile Application Architectures

When developing mobile applications, there are a number of key challenges where architecture and design are fundamentally different from that of a typical enterprise application. Careful consideration should be given to these mobile architecture issues early in the development process in order to mitigate the downstream impact of poor architectural decisions (Nilsson, 2008). The five most important areas for consideration, which are detailed throughout this document, include: performance, usability, data access, security, and connectivity (Sprunger, 2012).

Client/server architecture is the most popular architecture. However, some specific aspects related to the mobile devices (clients), and their connectivity with servers must be taken into account. There are many mobile device types, including RIM devices, cellular telephones, PDAs,

Tablet PCs, and Laptop PCs. These mobile devices can typically operate as thin clients or fat clients, or they can be developed so that they can host web pages.

2.7.1 Thin Clients

Thin client completely rely on the server for their functionality. They do not depend as heavily on the mobile device's operating system or the mobile device type as fat clients (Lee, Schneider, & Schell, 2010). The Twitter mobile application is an example of a thin client. The mobile application basically displays information pulled from the server. The information searches, image storage, media streaming all are handled by their APIs and backend processing.

2.7.2 Fat Clients

Fat clients typically have one to three layers of application code on them and can operate independently from a server for some period of time. Typically, fat clients are most useful in situations where communication between a client and server cannot be guaranteed. For example, a fat client application may be able to accept user input and store data in a local database until connectivity with the server is re-established and the data can be moved to the server (Lee, Schneider, & Schell, 2010). This allows a user to continue working even if he/she is out of contact with the server. An example of a fat client is *ePig*, a mobile application developed by Eclectics International to assist farmers to register their pigs and keep track of their feeding habits and their life cycle, from infancy all the way to piglet delivery. Due to network challenges in most farms, the above stated information is keyed in and stored in CSV file in the handheld device. When the internet connection stabilizes, the data is synchronized automatically with online servers

2.7.3 Server Architectures: Three-Tier Server architecture

Server architectures are commonly composed of one to three code layers implemented in one to three tiers. Three-tier architecture is typically composed of a presentation tier/user interface, a domain logic tier, and a data storage tier. It has the user interface, which runs on the user's computer (the *client*). The functional modules process data. This *middle tier* runs on a server and is often called the *application server*. The database management system (DBMS) that stores the data required by the middle tier runs on a second server called the *database server*. *Application*

using three-tier are scalable, secured behind firewalls and zones and allows database specialization.

Figure 2.4 shows the three tier server architecture

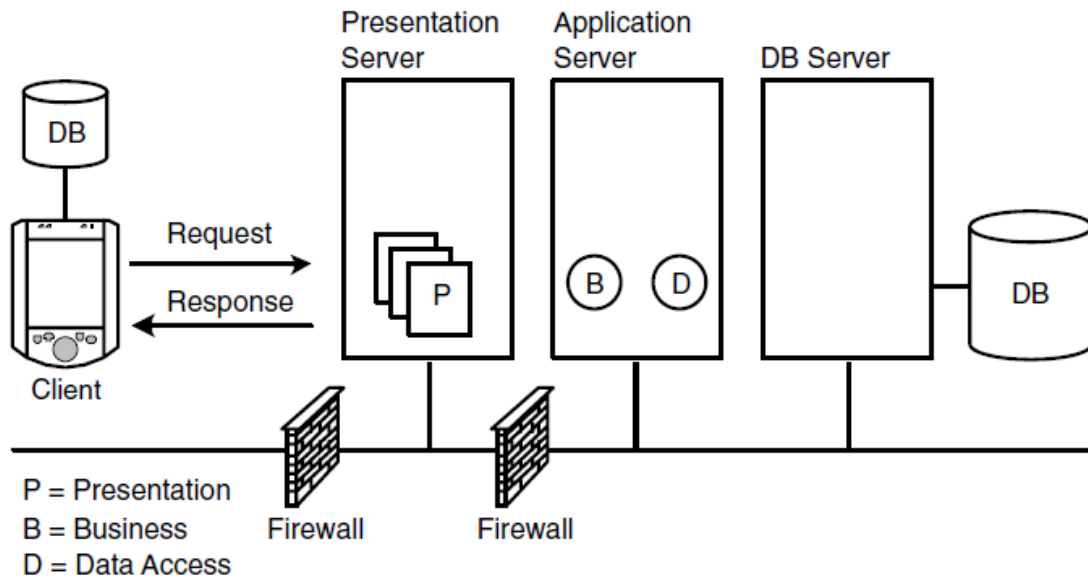


Figure 2-2: Three-tier server architecture (Lee, Schneider, & Schell, 2010)

Separating the presentation server and application server makes the architecture more expensive and complex to implement. Two-tier architecture makes a better option and is shown in Figure 2.5.

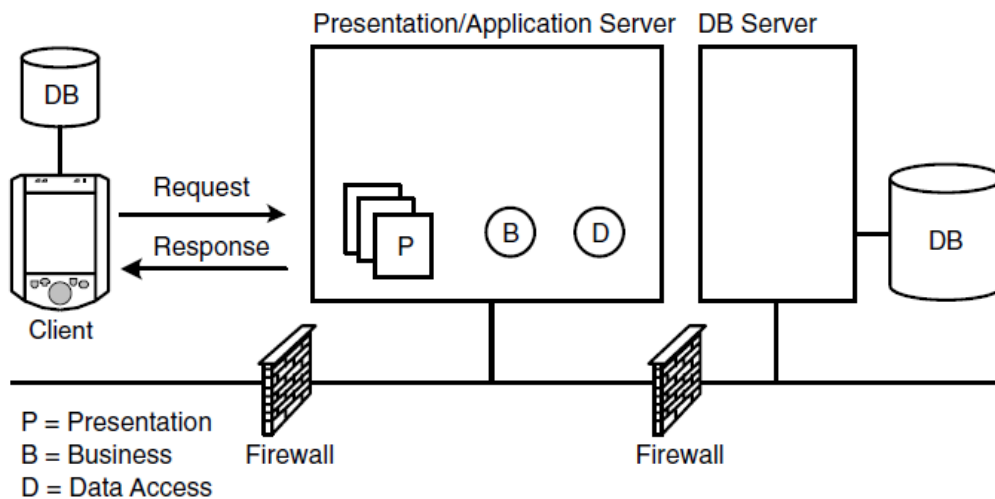


Figure 2-3: Two-tier server architecture (Lee, Schneider, & Schell, 2010)

2.7.4 Connection Synchronization

The connection type affects the way in which data can be synchronized between the mobile device and back-end systems. Synchronization is possible in two ways: continuously or through a store-and-forward method. When connectivity between a client and server cannot be guaranteed, it is still possible to store and transmit information safely using a method called “store-and-forward”. A mobile client application can initially store the data in a local database. Later, when a connection has been established, the mobile application will forward the data from the local database to the database on the server.

Figure 2.6 shows the store and forward synchronization

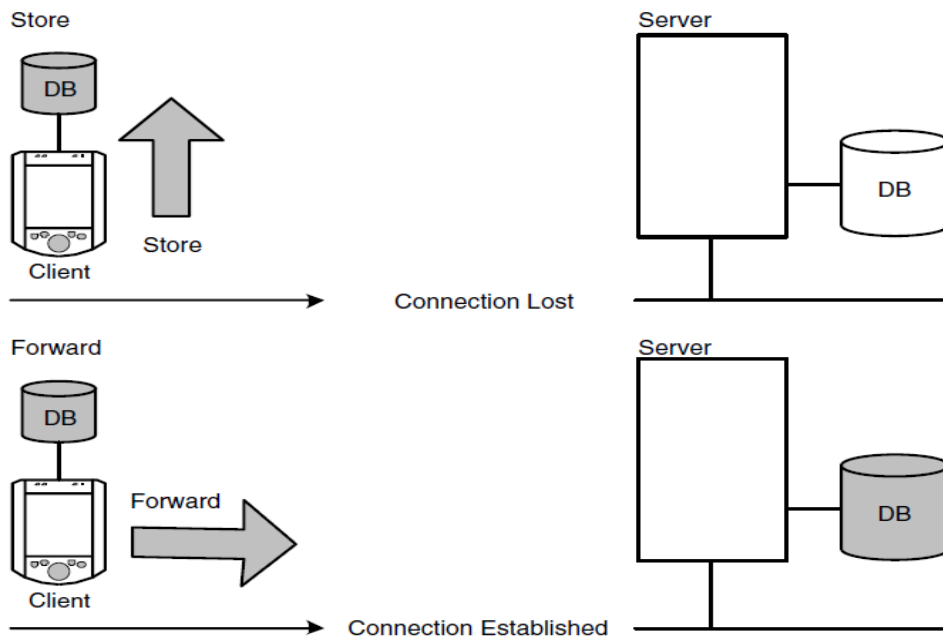


Figure 2-4: Store and Forward Synchronization (Lee, Schneider, & Schell, 2010)

2.7.5 Information Security

Information security is sometimes shortened as InfoSec. According to NIST (National Institute of Standards and Technology) (2011), Information security is defined as the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take; electronic or physical. The information that is collected about a crime is considered very sensitive. Therefore, the information must be secured while it passes to

the server on the networks. While it is stored in the database, there should be information access control mechanisms.

2.7.5.1 RSA Cryptosystem

The RSA cryptosystem illustrated in Figure below depends on a cryptographic algorithm based on two related keys. Demonstrating the existence of the algorithms and laying out the conditions that such algorithms must fulfil (Ogwueleka & Ocheme, 2014). It is therefore obvious that RSA algorithm encryption is an effective tool for protecting message from passive and active threats inherent in data communication.

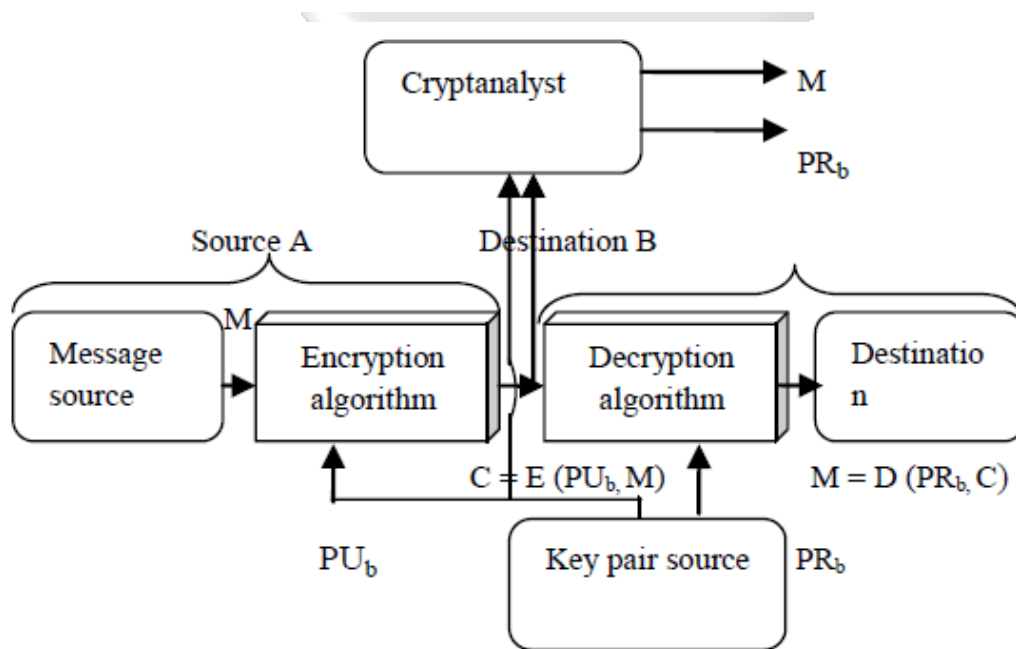


Figure 2-5: RSA Cryptosystem (Ogwueleka & Ocheme, 2014)

As illustrated above, the plaintext is extracted from the message as output M. Encryption and decryption processes entail the software generates the two keys, public and secret keys. The sender encrypts a message with the recipient's public key, while the recipient has to decrypt with his/her secret key to recover the message. There must be a message, mostly in the form of a plaintext, convertible to ASCII characters and vice versa, to be communicated between the two parties. The sender A must know the receiver B's public key and the message to be able to generate the cipher text. It is not feasible for a hacker, for instance, to know the receiver B's

private key from the public key. Neither will it be computationally feasible for an adversary who knows the public key and the cipher text, to recover the original text without knowing the private key (Ogwueleka & Ocheme, 2014).

2.7.5.2 Access Control

For security and control purposes, there is a restriction as to what information is available to which user category (Ogwueleka & Ocheme, 2014). For crime reporting application, tip-offs about suspected criminals uploaded to the server by the general public are not accessible to anyone, except the police. This is to prevent an incident whereby the criminal himself, through his handheld device becomes aware that, a tip-off has been sent about him to the police. Also, if a member of the general public sends a tip-off to the police, the sender's location information as well as his registration details are also recorded on the server for such sender's movement to be monitored at least for twenty-four hours by the police. This is necessary to prevent situations whereby criminals themselves deceive the police by sending false information to deceive and sway off the police (Agangiba & Akotam, 2013).

2.7.6 Crime Analysis and Mapping

According to COPS (Community Oriented Policing Services) (2001) crime analysis is the qualitative and quantitative study of crime and law enforcement information in combination with socio-demographic and spatial factors to apprehend criminals, prevent crime, reduce disorder, and evaluate organizational procedures (McCoy, 2012). Crime Pattern is the occurrence of similar offenses in a defined geographic area, usually defined by administrative boundaries. On the other hand, crime series is a crime pattern where there is reason to believe the same person(s) committed the crimes and crime trend is a recognizable general tendency regarding recurring patterns of crime which is revealed over a period of time. A trend may involve any one of the crime pattern factors or any combination of the factors.

There are three types of crime analysis; - administrative, strategic and tactical. Strategic crime analysis is used for identifying problems and potential approaches for dealing with them. Tactical analysis is used to take action designed to address specific types of crimes and

offenders. Administrative analysis is used for policy development and resource justification (McCoy, 2012). The basic process of crime analysis is shown in Figure 2.8.

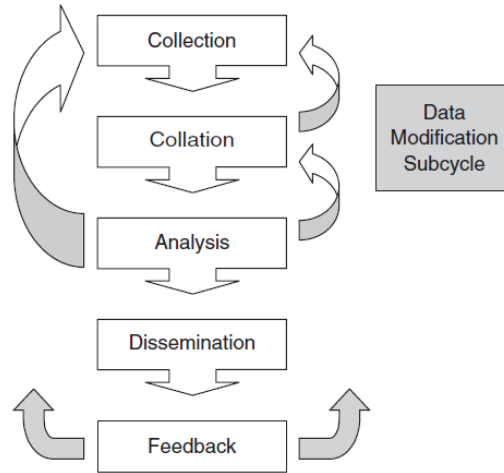


Figure 2-6: Crime Analysis Process (Crime Analysis Defined, 2005)

According to SHERIFF’S ANALYSIS GROUP (2015), representing reported crime rates for each year and for a number of years and trends is a result from good analysis. Figure 2.9 shows sample result from crime data analysis.

| UCR Part I Crime | 2013 | 2014 | Actual Change | % Change |
|-----------------------|---------------|---------------|---------------|---------------|
| Violent Crime | | | | |
| Homicide | 10 | 20 | 10 | 100.0% |
| Rape | 163 | 160 | -3 | -1.8% |
| Robbery | 554 | 447 | -107 | -19.3% |
| Armed Robbery | 256 | 209 | -47 | -18.4% |
| Strong Armed Robbery | 298 | 238 | -60 | -20.1% |
| Aggravated Assault | 2,132 | 1,805 | -327 | -15.3% |
| Total Violent | 2,859 | 2,432 | -427 | -14.9% |
| Property Crime | | | | |
| Burglary | 3,340 | 2,559 | -781 | -23.4% |
| Residential Burglary | 2,056 | 1,504 | -552 | -26.8% |
| Commercial Burglary | 1,284 | 1,055 | -229 | -17.8% |
| Larceny-Theft | 8,167 | 6,971 | -1,196 | -14.6% |
| Grand Theft | 3,315 | 2,681 | -634 | -19.1% |
| Petty Theft | 4,852 | 4,290 | -562 | -11.6% |
| Vehicle Theft | 1,797 | 1,563 | -234 | -13.0% |
| Total Property | 13,304 | 11,093 | -2,211 | -16.6% |
| Total Part I | 16,163 | 13,525 | -2,638 | -16.3% |

Figure 2-7: 2014 UCR Part I Crime (Source: ARJIS)

Wall maps have long been a simple and useful way to depict crime incidents or hot spots. Many police departments still have large maps tacked to the wall of the briefing room with the most recent crimes represented by pins. Although useful, manual wall maps, offer limited utility because they are difficult to keep updated, keep accurate, make easy to read, and can only display a limited amount of data (COPS, 2001). Because of this, online maps are very useful in mapping accident data. An example of this is Google map. Online maps are dynamic and have the capability to have different views. Crime information, which has location information, is fed to the maps together with other information. Markers can be used to carry the extra information (Google, 2012).

CrimeReports.com is a site used by Police of San Jose, California, USA to map crime information. Simply by clicking on CrimeReports.com and typing in a location, citizens can look at a Google Map that pinpoints exactly where police have responded to crimes within their neighbourhoods. Crime Reports works with thousands of law-enforcement agencies to help reduce, prevent and solve crime by enabling officials to easily open and manage a controlled dialog with citizens. Offering an online family of crime-fighting tools including a public crime map provided by Google Maps, alert messaging, anonymous tipping and data analytics. CrimeReports.com is a website that provides tools to help law enforcement agencies communicate directly with members of the communities they serve. Figure 2.10 shows sample crime data mapped on Google by feeding the crime data to Google Maps API (Google, 2012)

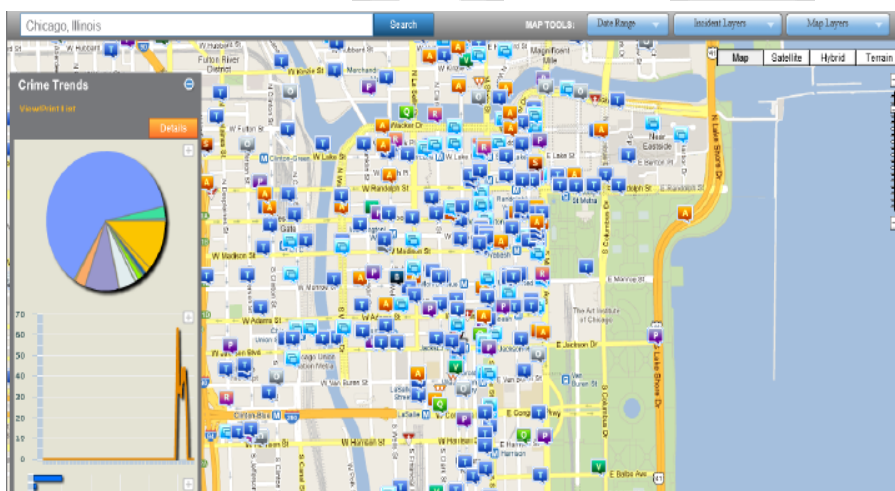


Figure 2-10: Mapped data on Google using Google Maps API (Source: Google, 2012)

2.8 Machine Learning and Artificial Intelligence

Machine learning is about looking at data and finding patterns, and such are the patterns that we human beings cannot detect easily. Before machine learning, we had rule based learning whereby we basically had rules that we evaluated one at a time to come up on a decision. Machine learning also involves some rule based learning but it does it in such a high dimension space that we cannot interpret them. Therefore, in this age of big data, it is a critical process to make sense out of a large amount of data.

2.9 Text Mining and Analytics

Text mining refers to the using of complex automated algorithms to learn and draw conclusions from a large dataset of texts. The sources of such texts can be from news articles or social media; for instance, Twitter and Facebook.

2.9.1 R and Azure Machine Learning Platforms

R is both a widely used programming language and development environment for statistical computing and data mining as well as graphical representation of the mined data, while Microsoft Azure Machine Learning platform is a managed environment for building analytic solutions and deploy as a web service.

2.9.2 Use of both R and Azure Machine Learning for Text Mining

In this research, both the Azure machine learning platform and the R analytics engine have been used, both in different contexts. The Microsoft Azure Machine Learning platform is used to interface to the Big Data services, and the cloud hosted SQL server database management system. The Azure platform is also used to provide a web service interface to allow external systems to interface to this environment.

This environment enables the possibility to run custom R scripts to further process the data. The graphs and plots that would have been plotted from the scripts are pushed back to the Azure web services that is ready for access with external systems.

2.9.3 Packages in Text Mining

The R programming language and platform, by itself is quite basic, and not sufficient to perform a conclusive data analysis. As a result, it allows the ability to add packages that perform specific

tasks, thus adding extra capability to the R environment. Below are the packages that were used during this research.

a. Hmisc

This is the Harrell miscellaneous library. It consists of many functions that are used for data analysis and high level graphics plotting. It is also responsible for character string manipulation as well as variable clustering.

b. FBasics

This is the markets and basic statistics library that aids with data that pertains, or takes the same structure as computational finance.

c. Mice

This is the Multivariate Imputation by Chained Equations library package, that has imputation models for continuous, binary and both unordered and ordered categorical data.

d. Ggplot2

This is the R package that is responsible for plotting graphs from multiple data sources

e. GridExtra

This is the package that comes in handy when multiple plotted graphs are needed to be arranged in a grid on one page or in a table.

f. Dplyr

This is a package that is used to work with data frames, both in memory and out of memory.

g. Reshape

While using just two of its core functions; cast and melt, this package allows the possibility to restructure and aggregate data.

h. NLP

This is a package contains the basic functionality for Natural Language Programming

i. TM

This is the Text Mining package, which has the methods and functions for text mining within the R platform

j. SnowballC

While using the Potters algorithm for word stemming, this package is able to get the root word for most words in various languages. This is important in text mining for vocabulary comparison.

k. Rcpp

This is the R package that provides the seamless integration between the R programming language and C++ programming language, thus allowing easy integration with third party libraries that are in C++

l. Wordcloud

This is a package to draw a word cloud that can be used to graphically represent frequency in words.

m. Magrittr

This is a package provides a way to chain commands while using a forward pipe operator “%>%.”

2.9.4 Term Document Matrix and Document Term Matrix

These are both two dimensional matrixes used in information retrieval in large sets of text documents. In the former, the terms are the rows and the documents are the columns while in the latter, the rows are the documents.

Putting into consideration a corpus of documents and a dictionary of terms that do appear in these documents, each entry in this matrix shall represent the frequency of the term in each document. Due to the varying complexity between adding a column versus adding a row, each of the above matrixes has a context in text mining where one is preferred over the other.

2.10 Synthesis and Gaps in Literature Review

From the forgoing, it is clear that Nairobi and Kenya in general is insecure, with a low safety index of 21.01. The police are responsible for responding to crimes reported. However, this literature review has shown that the methods used are not appropriate because they are not timely. It is clear that penetration of smart phones in Kenya is high and most users can access Internet on their phone and are savvy enough to use any mobile applications. The crime reporting mobile applications that have been successful elsewhere in the world use different mobile platforms. Android OS is the most popular smart phone OS in Kenya. In addition, the other applications discussed above have only been suited to their respective countries or regions.

We note that securing crime information while on transit and in store are very crucial. The applications described above do not indicate how data is protected. The use of RSA cryptosystem in securing data in transit in networks is a motivation to this study. The solution suggested by Agangiba and Akotam is a crucial motivation for this study. From the light of this literature review we propose a crime reporting mobile application with the following properties:

- Run on Android platform.
- Use two-tier server architecture .
- Use store-and-forward connection synchronyzation.
- Use RSA cryptographic alogorith to protect crime tip-offs while transiting on networks.
- Use access control to ensure that the right people see the crime information.

Chapter 3 : Research Methodology

The literature review has put this work into context. In the literature review, the researcher effectively finds information about the current security problems and how mobile technology can be used as a solution. In this chapter, the researcher explains the meaning of research methodology, and then explains the procedure followed to design the proposed solution. The main method used to collect data is material review and therefore, it dominates the content of this section.

3.1 Research Design

According to Katherine(2005), research design is a step-by-step plan that guides data collection and analysis. In the case of secondary data reviews it might simply be an outline of what you want the final report to look like, a list of the types of data that you need to collect, and a preliminary list of data sources. The types of secondary materials that may be used to conduct a research will always depend on the focus of the research, and what results are expected at the end of the research. Secondary data analysis and review involves collecting and analysing a vast array of information.

Normally, a material review, which is done in the literature review, must answer a number of objectives. The materials reviewed in this work were obtained from institutional data and research that has been done in the past. According to Katherine(2005), the choice of a material to be reviewed depends on the original purpose of the work done, credentials of the material author, the intended audience, date of publication, quality of references used and if the methods used to collect the data are sound. All these factors were taken into account while choosing the materials that were reviewed.

3.2 Location of Study

The location selected for the study was Nairobi County. The county was selected since it is the capital city, most of the population has smart phones and it is the county with the most crime incidences. The study focused on observing current trends that occur in reporting crimes and analysing crimes. Nairobi County provides a good location to perform the research as most of the citizens have smart-phones and it would be a good place to research on the criminal activities.

3.3 Data Collection

The study used both primary and secondary data collection methods. The data was collected through the use of document review and user input from the mobile application. The following research instruments were selected as they provided precise information, which provided transparency and accuracy in answering the research questions.

3.3.1 Mobile Application Input

The mobile application provides forms to the users, to allow them to submit suspicious activities categorised into five major categories. These include suspicious persons, vehicles, places and incidents. In addition, a fifth form for submitting emergencies is made available to the users.

3.3.2 Document Reviews

A review of technical reports provided research results of projects that have been done. Most of reports were about projects, which have been done. Scholarly journals provided original research and experimentation written by experts in specific fields. Articles in scholarly journals usually undergo a peer review where other experts in the same field review the content of the journals for accuracy. Literature review articles were reviewed as they contained an assembly and review of original research dealing with a specific topic. These were written by experts in the area of mobile solutions and discussed all the relevant publications in the area of interest.

Reference books provided secondary source material. More often, the books contained theoretical information about certain concepts. Official statistics were used to give figure about facts; for example, the safety index of Kenya. Product websites in the literature review, discussed about crime applications that are already working. The websites for such products were a good source of information.

3.3.2.1 Experiments with Mobile Applications in Play stores

The researcher made experiments with existing mobile applications regarding security that were in the play stores. The play store that was used was the Google play store due to its popularity by customers and due to the fact that it only displays mobile applications developed in android platform. The focus of this work is to propose a mobile solution on android platform, which will be used to report crimes. Most of the applications reviewed were in the play store and more information was obtained from the application developers.

3.4 Data Analysis

i. Data input

In this research we are getting data directly from the SQL database where all the reports are stored. These reports are a collection logs pertaining to suspicious persons, vehicles and occurrences.

Data cleaning:

Here the columns and rows that may be noise to the analysis are removed. In this research we are going to set empty columns to null and omit the index id columns.

Data split:

Upon having this dataset in place, the data is going to be split into training and test datasets. Training dataset is what shall be used to train and therefore build the model, and then test the model using the test dataset. When a model is being created, relationships get created between the various columns.

Therefore, the main reason for splitting the dataset is to see how the model shall perform on the test data, which shall be the data that it has never seen before. This way the efficiency of the prediction is put to test and analysis of the model is done determine whether its values can be trusted while in production.

In this research the data is split in rows while allocating 80 percent of the rows in training the model and the remaining 20 percent for testing the models prediction and analysis accuracy.

3.5 Validity and Reliability

Once the data has been imported, the design of the model that shall be used for machine learning starts. During this stage, there are three critical steps involved. They are the training step, scoring step and evaluation step. The models performing these activities are Train Model, Score Model and Evaluate Model respectively.

i. Training

In the training step, the Train Model is initialized with an algorithm of choice. However, the choice of algorithm that is going to be used to build a model is dependent on the data you are working with, and what is the expected nature of result from the model, and what is being tested.

During this research a combination of Multiclass Neural Network algorithm, and Logistic Regression shall be used. The former is to establish the relationships between the various data provided to predict the name of the suspect. The latter is to provide statistical information regarding the data.

ii. Scoring

The result of the Train Model and the test dataset are going to be tested and scored on the Score Model. The Score Model scores the accuracy of the prediction and analysis. It does this by the notion, *given this suspicious persons dataset, this is what the Train Model produced and this is what the answer was, in the test dataset.*

iii. Evaluation

Finally the Evaluate Model takes this data and makes some summary statistics on top of the result so to evaluate how good the Train Model performed.

3.5.1.1 Model to Production

After the tests yield desired results, we save the model and put it into production. The model in production can be in form of a service or an API. Figure 3.1 shows the graphical representation of the machine learning life cycle.

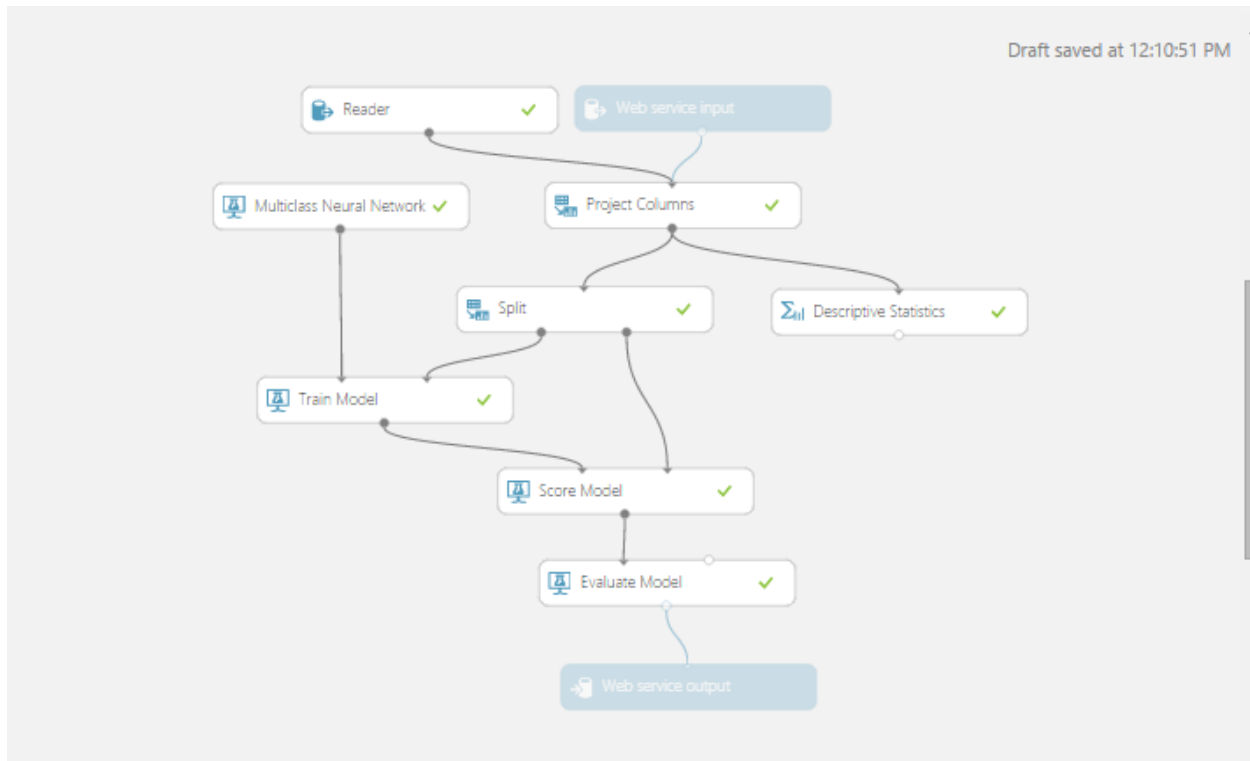


Figure 3-1: Machine Learning Life Cycle

3.6 Quality of the Research Instruments

3.6.1 Efficiency

Machine learning give answers in different forms. The first form is Boolean in nature, for instance Yes/No, or True/False form of answer. The second form is the multiclass type of answer, for instance (A, B or C) or (Red, Blue or Green). The third form is an answer that is a number, perhaps when we are trying to predict what might be the projected sales in the next four years. Finally, the answer can be in form of a probability. This form also is used in conjunction with the previous three, in such a way that it is how probable the machine learning thinks whatever answer given is right.

Therefore, not only does machine learning give answers, but also a probability of how good it thinks that answer is.

3.6.2 Reliability

Machine learning uses other pieces of information to predict other pieces of information in a particular dataset. One approach can be specifying the columns of data to be used to predict a particular column value. In machine language the above mentioned columns are referred to as class and target column respectively.

Consequently, machine language is very reliable since you can feed it with a large amount of data in a dataset and it will try to find a way of predicting any missing column value, given the rest of the information.



Chapter 4 : System Design and Analysis

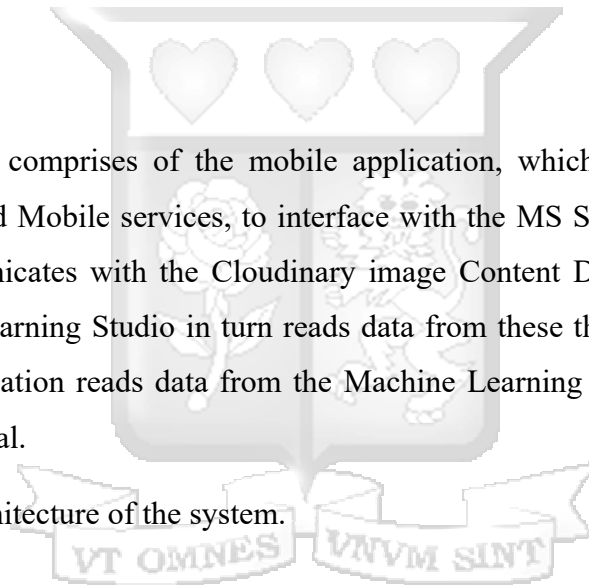
The discussions of the research were guided by the research objectives and the research questions. The research sought to investigate the viability of having a mobile application that would use artificial intelligence to analyse and categorize data that has information on criminal activities, reported by Kenyan citizens. In order to design and develop a mobile application to allow users to report criminal activities occurring in their vicinities the system analysis was performed and various diagrams such as use cases and others were drawn and detailed information for each design was illustrated. This chapter presents the design of data mining and analytics system. It also looks at the findings and results on how the machine learning model performed as well as mining and analysing the data.

4.1 System Design

System Architecture

The system architecture comprises of the mobile application, which communicates with the Microsoft Azure API and Mobile services, to interface with the MS SQL database. The mobile application also communicates with the Cloudinary image Content Delivery Network to store images. The Machine Learning Studio in turn reads data from these the MS SQL databases for analysis. The web application reads data from the Machine Learning services and displays the analytics data on the portal.

Figure 4.1 shows the architecture of the system.



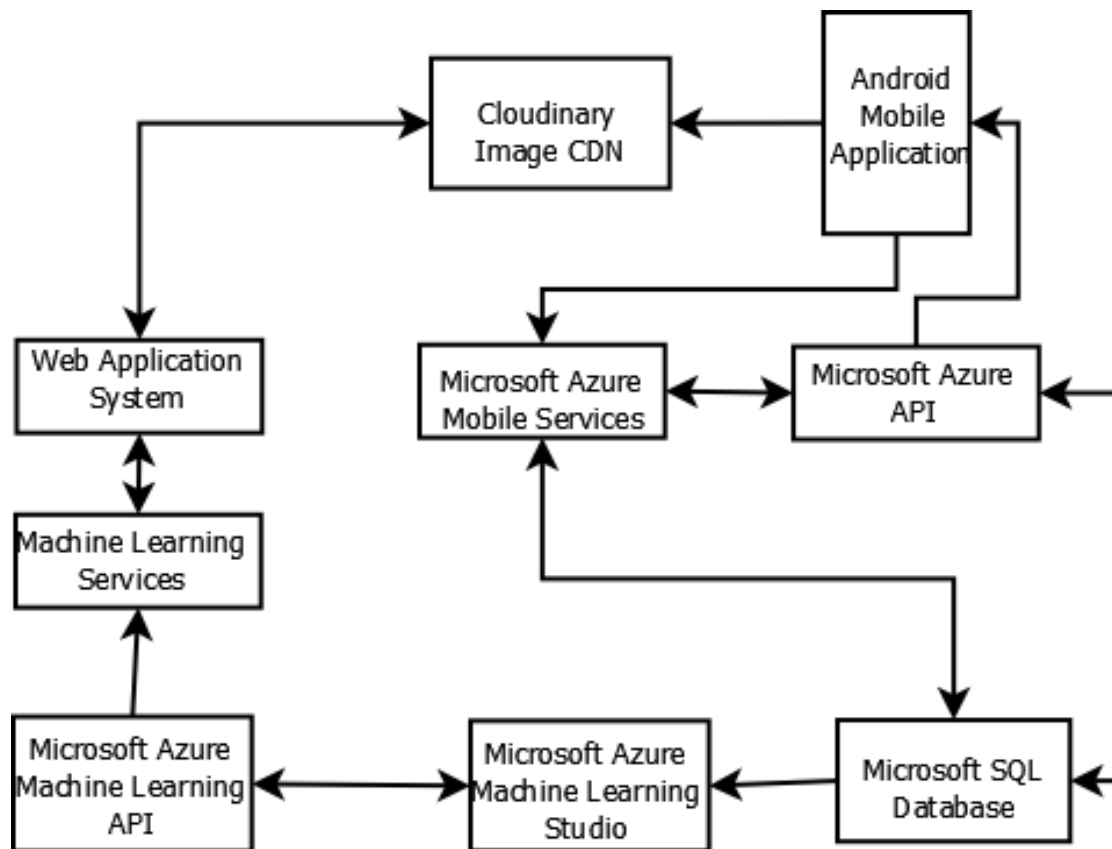


Figure 4-1: The System Architecture

4.1.1 Client Side

The client side consists of an Android based mobile device. It is from this device that the general public shall be able to submit reports on any suspicious persons, vehicles, incidents and places, as well as receive some requests from the web portal.

4.1.2 Server Side

The server side is a web based admin portal that shall have access to the logs of the various type of data submitted by the users from their mobile applications. The server side shall have a provision to send requests to the client side as they request for more information.

The Microsoft Azure Machine Learning platform shall be accessible from the server side web application only to receive analysed data.

4.2 Data and Process Modelling

4.2.1 DFD Models

The data flow diagrams will be used to show how the data moves through the system.

Figure 4.2 shows a Level 0 DFD of the system

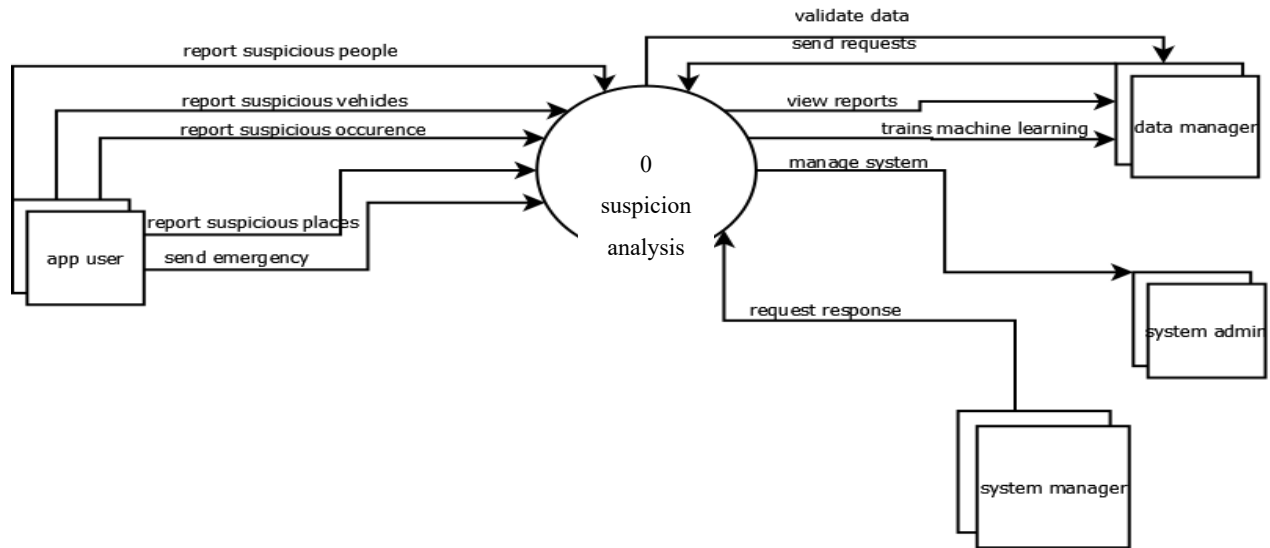


Figure 4-2: Level 0 DFD of the System.

Figure 4.3 shows a Level 1 DFD for the system. The diagram shows the various sub processes that make up the system. The flow of information among the various entities is shown.

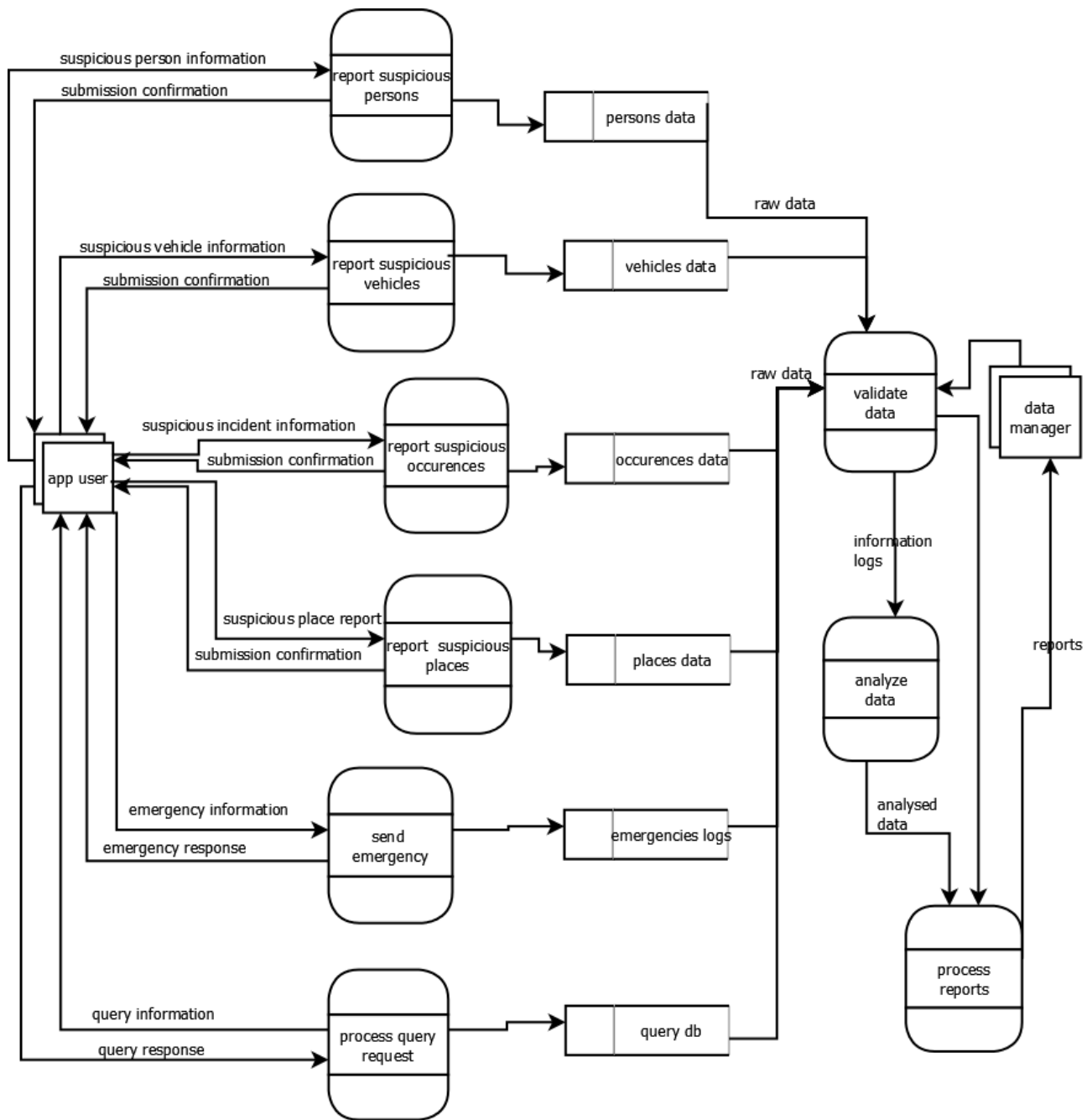


Figure 4-3: Level 1 DFD

4.2.2 Use Case Modelling

Use case diagram describes how the main users of the application interact with the system. The mobile application does not require any registration; therefore any person can use it to submit any information that raises their suspicion about their security. Figure 4.4 illustrates the use case diagram

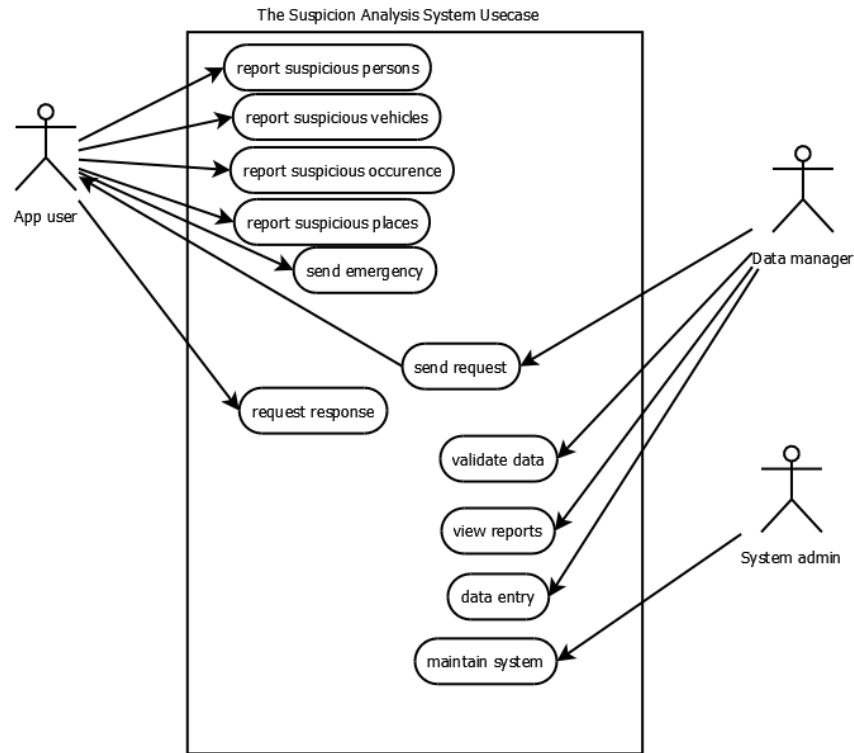


Figure 4-4: The Use Case Diagram

4.3 Database Design`

The database design of the system consists of two components. The relational database schema and the NoSQL schema.

4.3.1 The Relational Database Schema

The relational database schema, firstly consists of tables that correspond to the five components of the application; namely, suspicious persons, suspicious vehicles, suspicious places, suspicious occurrences and emergencies. Secondly the tables that shall store the information that has been pre-processed by the message splitting APIs. Thirdly, the admin portal tables. Fourthly the tables that pertains to the news feeds and warnings the administrators send to the public and finally the reference tables. Figure 4.5 shows how the database design and how they relate to each other in the system.

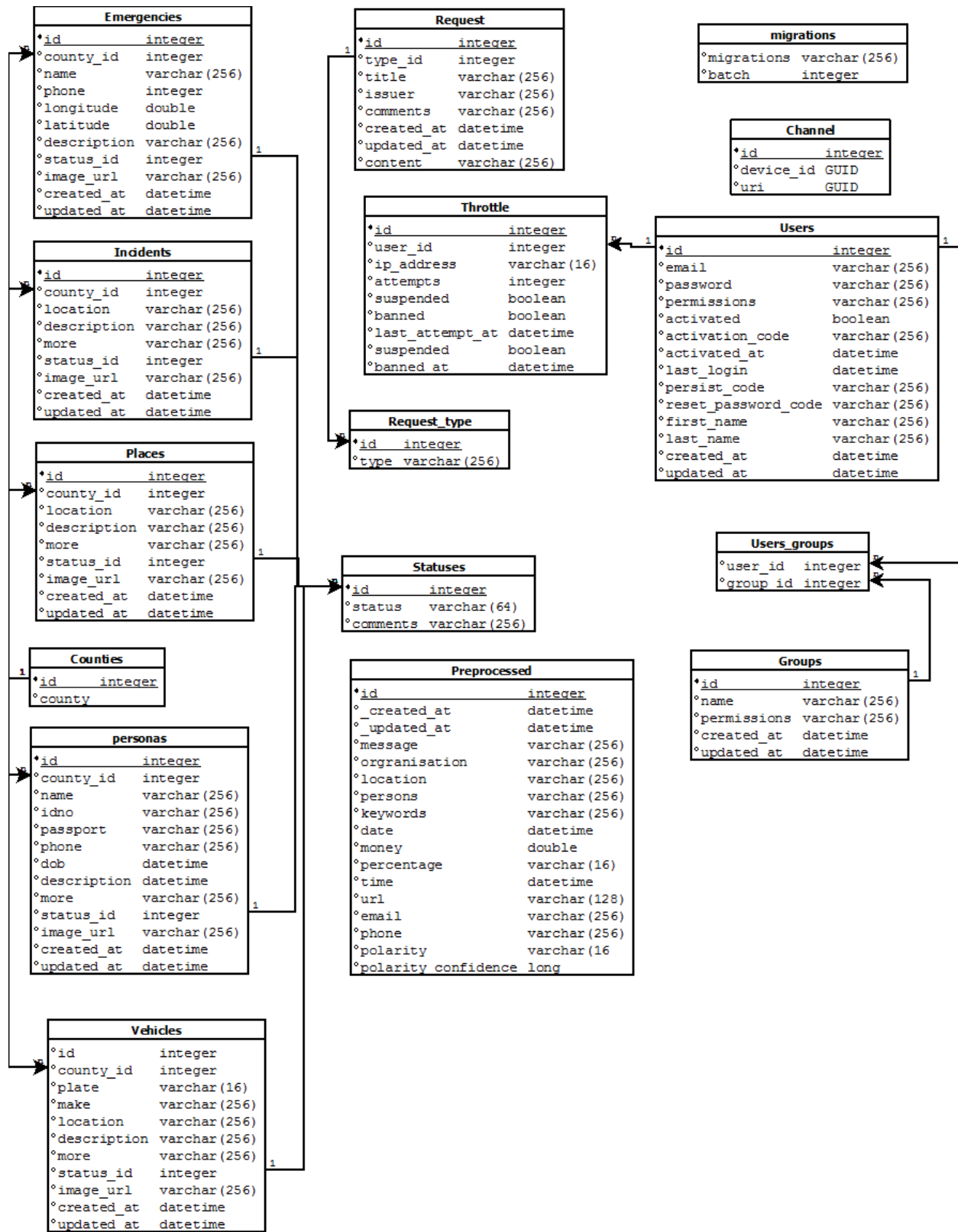


Figure 4-5: The Relational database design

4.3.2 The NoSQL Database Schema

The data is first stored in their relevant tables before pre-processing. The text processing API segments the combined data into various categories and places each category in its own column. These categories are:the original message, organisation, locations, persons, keywords, date, money, percentage, time, URL, email, sentiment Polarity and confidence of sentiment polarity.

Amongst these categories, the NoSQL database schema also stores a row for the PartitionKey and RowKey. The RowKey is a unique GUID generated on data entry and PartitionKey refers to this particular schema. Another schema would have a different PartitionKey.

Figure 4.6 shows how the database design and how they relate to each other in the system.

| TableStorage | |
|----------------------|--------------|
| *PartitionKey | GUID |
| °RowKey | GUID |
| °id | integer |
| °_created_at | datetime |
| °_updated_at | datetime |
| °message | varchar(512) |
| °organisation | varchar(128) |
| °location | varchar(128) |
| °persons | varchar(128) |
| °keywords | varchar(512) |
| °date | datetime |
| °money | double |
| °percentage | varchar(64) |
| °time | datetime |
| °url | varchar(128) |
| °email | varchar(128) |
| °phone | integer |
| °polarity | varchar(16) |
| °polarity confidence | long |

Figure 4-6: The NoSQL database design

4.4 Security Design

The information that flows throughout the system is secure and encrypted. The communication between the mobile application and the web based system is via a HPPS based API. The end points of this middleware are data encrypting libraries provided by the Azure Mobile Services software suite and enforced by the use of session keys for authorization.

The database server is hosted on the Microsoft Azure Cloud Database, which is IP restricted so that only the web portal can access it and from a particular pre-defined IP address.

The NoSQL database schema is stored on the Machine Learning platform, with a one off password that is auto generated from its administration portal, can be accessed via public key SSH.

4.4.1 Analytics and Machine Learning

This component consists of Microsoft Azure Machine Learning platform that makes the relationships, analysis and prediction on the information stored in the system.

4.5 Text Mining and Analytics

4.5.1 Introduction to Text Mining

Text mining refers to the using of complex automated algorithms to learn and draw conclusions from a large dataset of texts. The sources of such texts can be from news articles or social media; for instance, Twitter and Facebook.

4.5.2 Reading the Data

Data can be read from CSV or PDF document that may have been uploaded to the environment via a zip file, or data that has been stored remotely and accessed via a secure connection. During this research, the data is stored in the NoSQL data tables after the pre-processing that was done before storing the data

The data is stored in NoSQL data tables to harness the power and efficiency of big data in analytics. The environment used for the data analytics is the Microsoft Azure Machine Learning, and it connects to the data storage through the input data node as illustrated below. Credentials are provided to the node and it gets all the data in one go, together with all the columns.

4.5.3 Pre-processing of the Read Data

a. Removing unwanted columns

Since not all the data is needed, a need arises to choose the columns that are needed for data analysis. This is done by the column select module as illustrated below. The partition key and row key, which exist as a unique GUID of each row are removed at this stage of pre processing

b. Removing duplicate rows

There are scenarios where the data might be posted multiple times by the user and multiple copies of that information ends up existing in duplicate. Therefore, as a part of pre-processing already stored data, duplicate rows are removed by the module as illustrated below.

c. Clean missing data

For each report reported by the users of the mobile application, not all the form fields are mandatory, and therefore such columns of this records are stored as empty. Such empty rows might bring inconsistencies with text mining. As a result there are two scenarios that can be at play, either the rows with missing data to be deleted, or the missing data to be replaced by a place holder. In during this research, the missing data was replaced with NA for categorical data, and the integer 0 for numerical data.

d. Perform descriptive statistics

At this stage, the pre-processing of the data that has been read from storage is complete, and ready to be handed over for analysis with the R platform. To ensure that the data has been well pre-processed, we perform descriptive statistics on this data to confirm all the pre-processing has been performed successfully. Sample of the results of this stage are as illustrated below.

4.5.4 Sourcing data into the R platform

While using the R container module of the Azure Machine Learning platform, an R platform is created to perform further data analysis beyond which the Azure platform can provide. Each R container has two input ports for the data.

The pre-processed data above is read into the R platform while using the first input port. It is at this point that the strings in the data, that are by default considered as vectors, are changed to characters.

4.5.4.1 Converting data to data-frame format

The read data is converted to something called a data-frame. A data frame is a basic data type in R that just stores a table of data. The variables, what is commonly referred to as the columns, can contain a mixture of data types. It is a list of vectors of equal length.

4.5.5 Data Pre-processing

Despite having done some pre-processing of the data with the Azure platform, there are other pre-analysis processing on the text that takes place in the R environment. These are performed on the created corpus and are elaborated as below.

a. Simple transformations

Due to forthcoming validations below like removing punctuation and stripping whitespace, some simple transformations are performed as a preliminary step. These include replacing some characters like the slash “/” which separate alternative words with a blank space. This is because it would be removed during the removing punctuation step and the two words would be merged to one. It is for the same reasons that we remove the pipe symbol “|”.

This is achieved by the *toSpace* functionality in the *tm* library explained earlier

b. Conversions to lowercase

All the text in the corpus is converted to lower case to avoid having variations of the same text or word as a result of different case. This is important to avoid repetition.

This is achieved by the *content_transformer* functionality in the *tm* library, while passing the *toLower* argument to it.

c. Removing numbers

As part of a standard text mining exercise, numbers are removed to improve on the text mining analysis. However, in this particular context our data contains number plates and phone numbers and dates. As a result, this step was omitted during this research.

d. Removing punctuations

During this research, punctuations were removed. Despite punctuation providing meaning to a normal reader, in text mining punctuation may create variations of the same term. In addition, this step provides ease for the word stemming step below.

This is achieved by the *removePunctuation* functionality, also in the *tm* library.

e. Removing stop words

Stop words are common words that are used in grammar but add no value in text mining. In English, examples of these include; *very*, *and*, *too*, amongst others.

This is achieved by the *removeWords* functionality, also in the *tm* library, while passing *stopWords('english')* as an argument.

f. Removing dirty works

To improve efficiency in text analysis, we have to entertain the possibility of the users of mobile application to key in useless data, potentially dirty words. We load a list of commonly known profanity words and remove such from our text analysis.

This is achieved by specifying them as custom stop words and passing this list to the *removeWords* functionality as an argument, instead of passing *stopWords('english')*.

g. Striping whitespace

Whitespace is tripped off the text to improve the efficiency of creating the term document matrix. This is achieved by using the *stripWhitespace* functionality in the *tm* library.

h. Customised transformations

Despite the removing stop words and dirty words, we are going to perform additional text transformations. This is done primarily to yield a better term document matrix. These additional transformations include transforming to abbreviations, commonly used slangs to English words.

- Republic of Kenya to Kenya
- Kenya Police to Police
- Criminal Investigation Department to CID
- “*Karao*” commonly used slang of police, to Police

i. Stemming

The word stemming step is important to get the root words for better term document matrix. This step makes words like stole, stealing and steals all to be converted to the root word steal.

4.5.6 Term Document Matrix and Frequent Terms

The term document matrix is created after all the above transformations have been done, to yield a more useful term document matrix. Term document matrix shows the frequency of the terms in the relevant texts in the corpus.

From this matrix we are able to plot a graph demonstrating the most frequent term that is occurring in this analysis. This can be made useful to capture a trend of a particular crime. The term frequency plot is as illustrated in section 4.2.

4.6 Machine Learning and Prediction

4.6.1 The Raw Dataset

This is the raw dataset before analysis. Figure 4.7 shows a sample raw dataset. This is the scope used; it has six hundred and thirty four rows of records. It has also details regarding suspicious people whom the public has reported. The information includes names, national identification numbers, passport numbers, phone numbers, their description and a reason why they seemed suspicious.

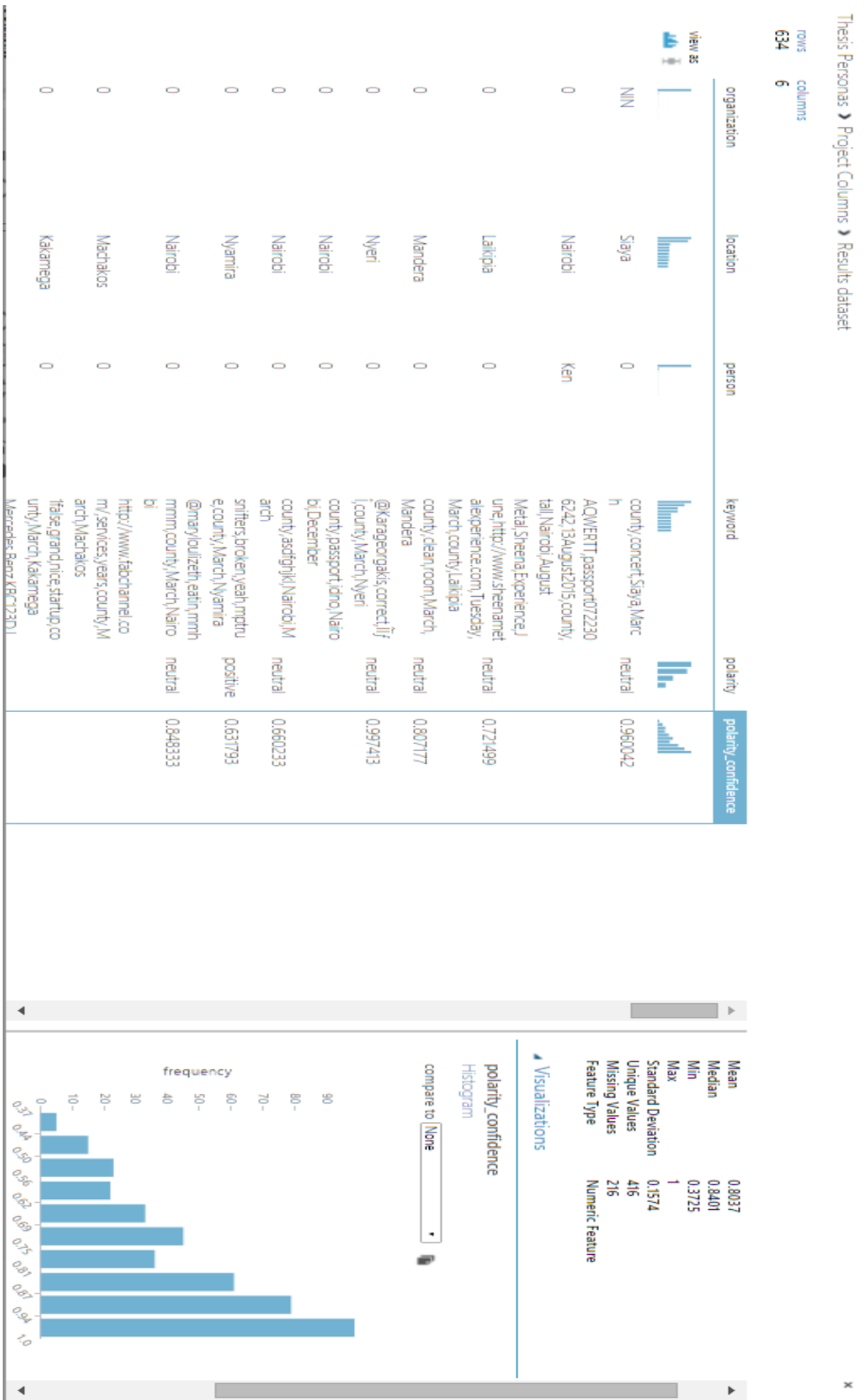


Figure 4-7: The Raw Dataset

4.6.2 The Split Datasets

a. The Training Dataset

Figure 4.8 represents the training dataset after splitting the initial dataset to get the test dataset and the training dataset. As indicated it has 507 rows. The other 127 rows have been reserved for testing this training dataset. The splitting was done on a ratio 4:1. More rows were given for the training dataset to make it more accurate in predictions and analytics.

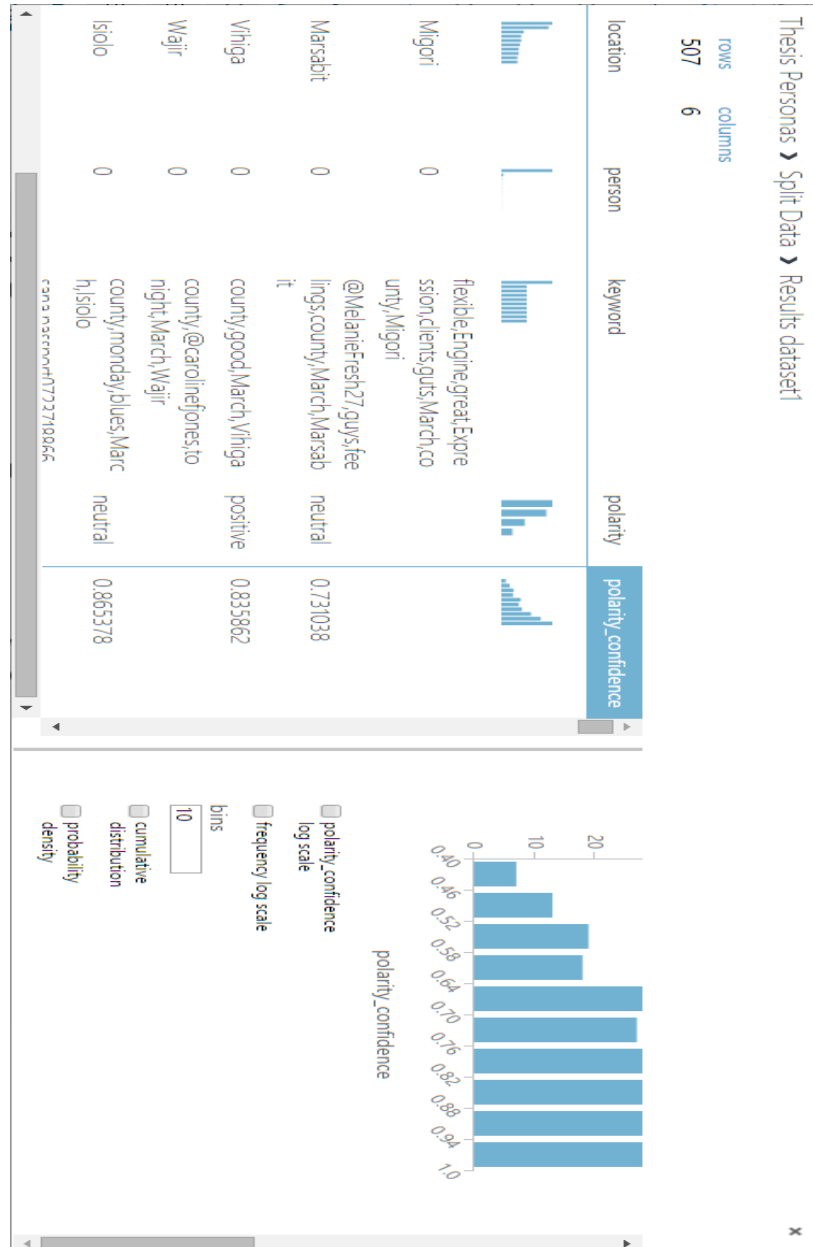


Figure 4-8: The Training Dataset

b. The Testing Dataset

Figure 4.9 represents the testing dataset and it has 127 rows, the other rows are being used as the training dataset as explained above. This is what shall be used to test the trained model.



Figure 4-9: The Testing Dataset

c. The Score Model

Figure 4.10 below shows the score model. It has indicated the scored label and the various scored probability per test class. From the presented data, it could determine what the test data was, with the below shown probabilities.



Figure 4-10: The Score Model

d. The Evaluate Model

Figure 4.11 shows the Evaluate Model, as well as the true positive plot and the extents to which the results were deemed accurate during the prediction training exercise.

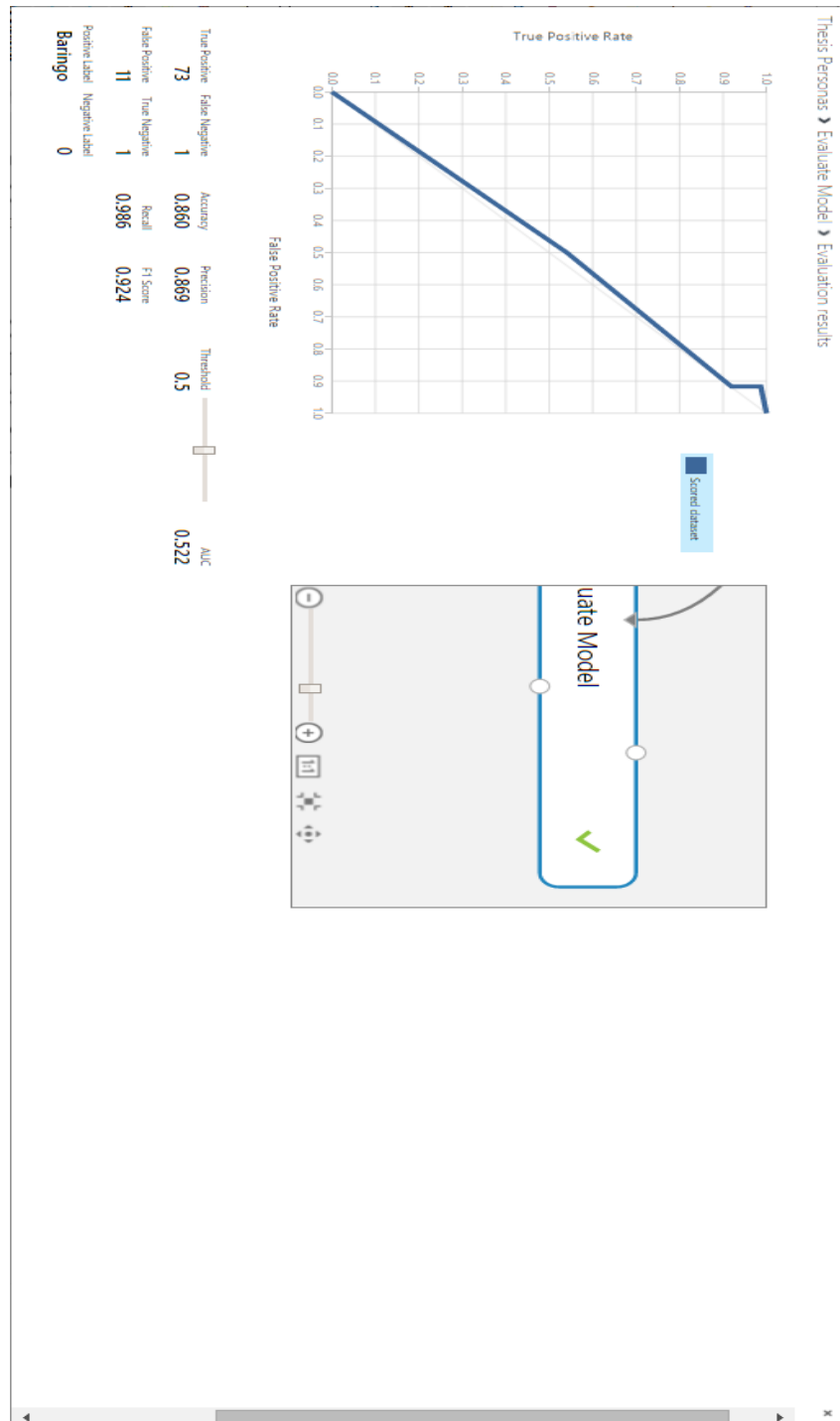


Figure 4-11: The Result of the Evaluate Model

Distribution of location by polarity

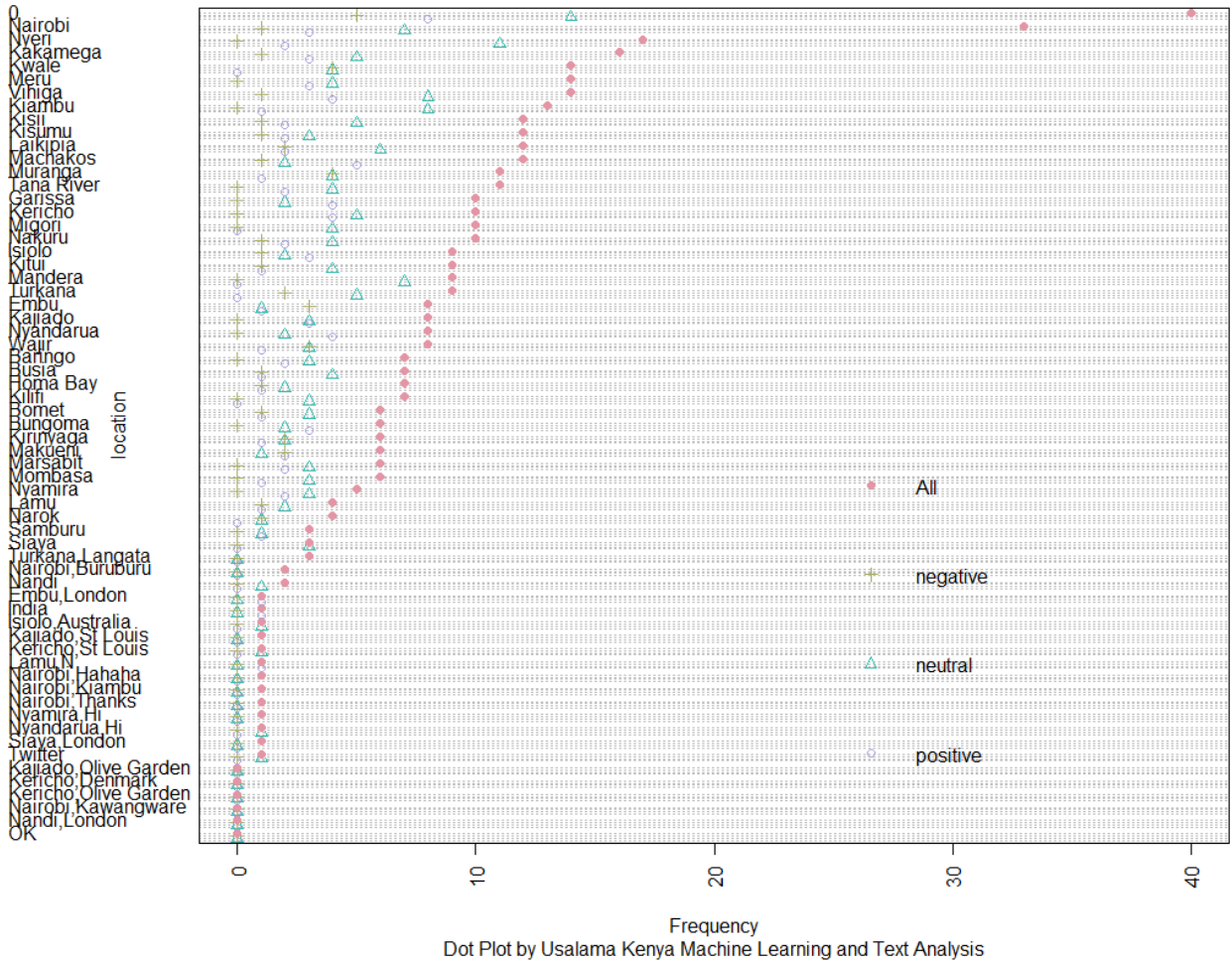
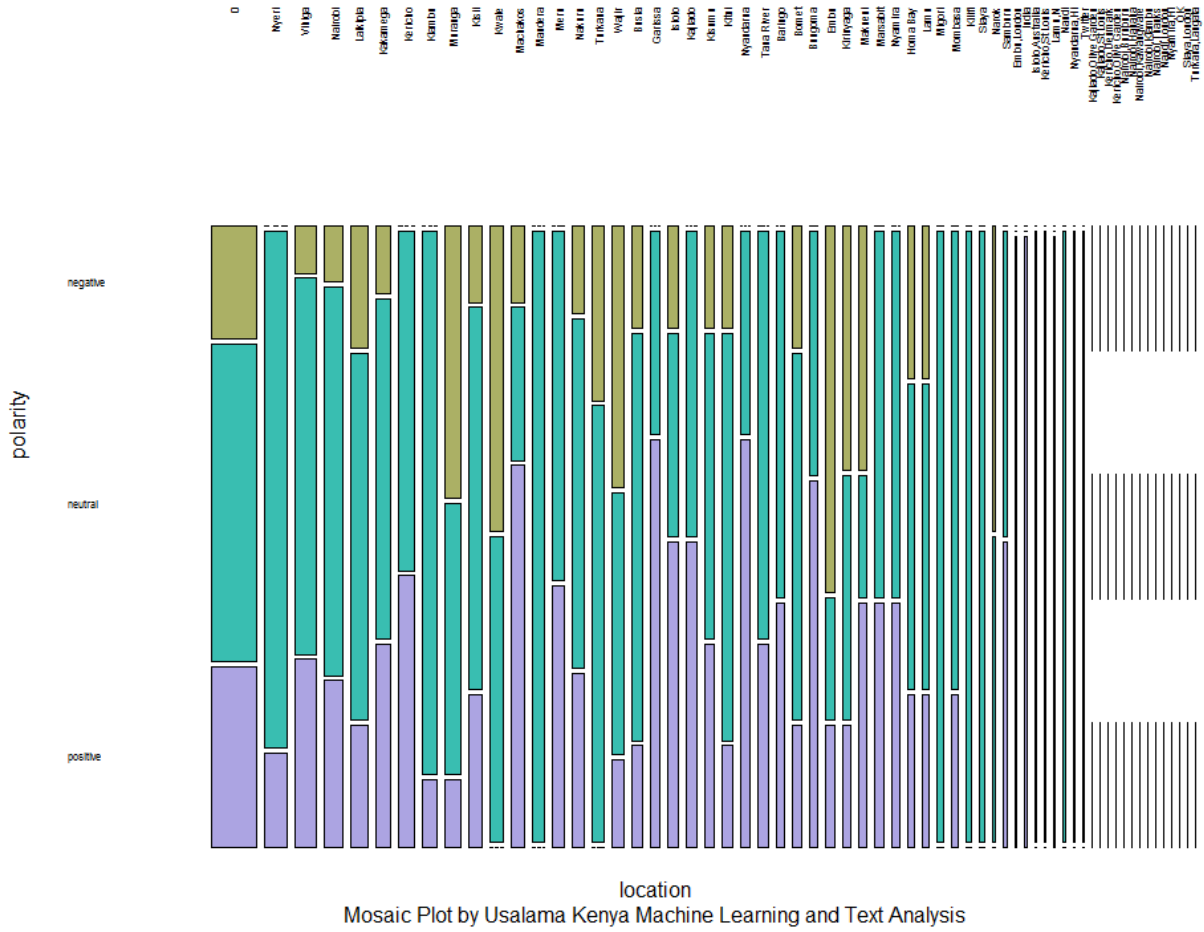


Figure 4-13: A Dot plot illustration of the distribution of location by sentiment polarity

Mosaic Graph of location by polarity



VT OMNES VNVM SINT

Figure 4-14: A Mosaic plot illustration of the distribution of location by sentiment polarity

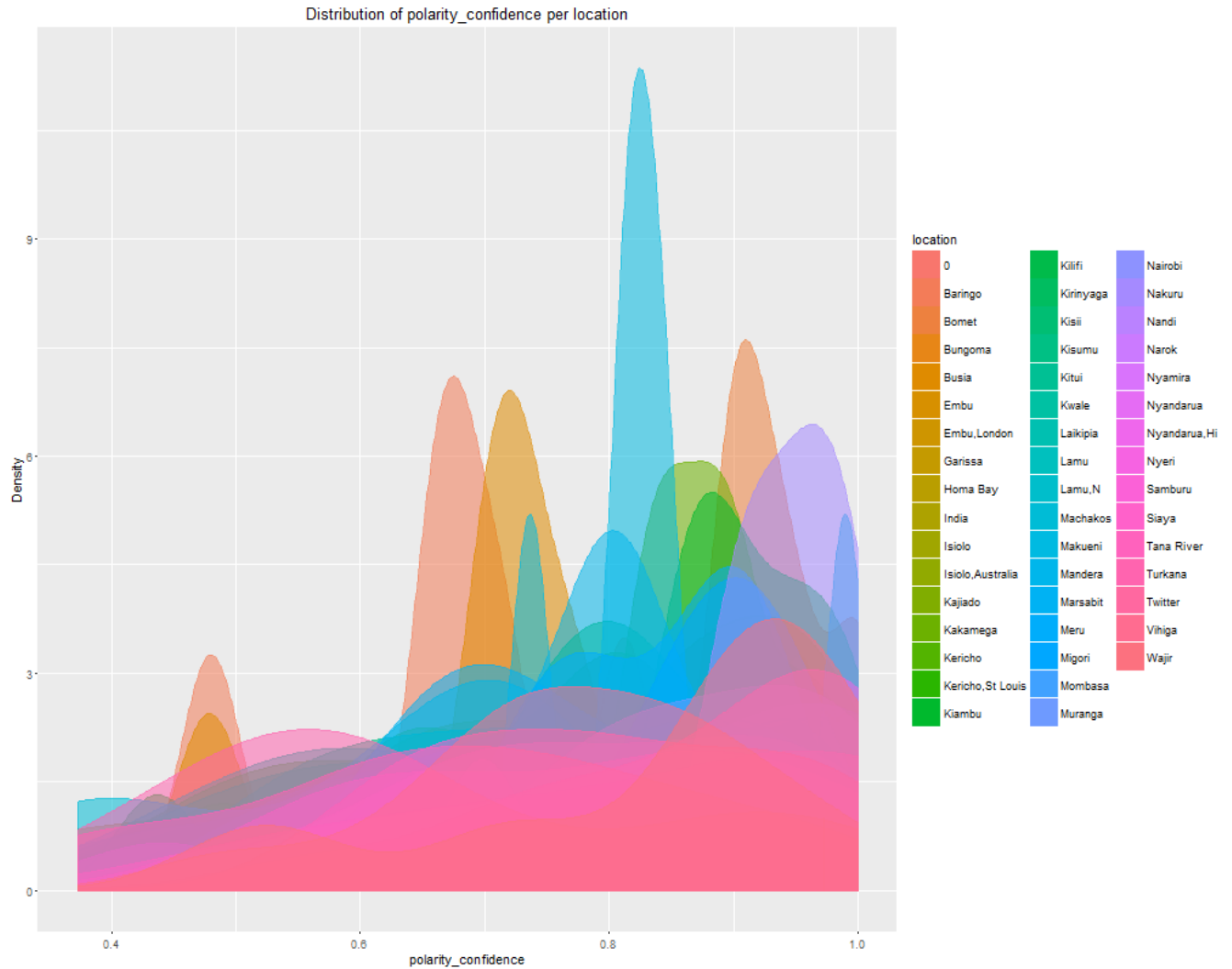


Figure 4-15: A histogram illustration of the distribution of location by sentiment polarity

4.7.2 Distribution of Persons

During the text mining analysis information, persona data was mined from the information that was submitted by the users via the mobile application. This data is later visually represented into various plots and charts in the web application for quicker understanding of the data.

The Figure 4.16 shows the bar plot of persons versus the sentiment of the information that was submitted via the mobile application. This data has the frequency of the persons, together with the average sentiment polarity of the person as per the context of reporting that includes the levels of positive, neutral and negative. This makes every reported person information have four-

bar group per person. From the illustration, the messages that mentioned the person ‘MercedesBenz,Francis’ were reported the most, whereas the ones pertaining to person ‘Damn’ had the most distress than other persons. The Figure 4.17 and Figure 4.18 illustrates the dot plot and Bedford’s law digital analysis plot respectively for the same data explained above

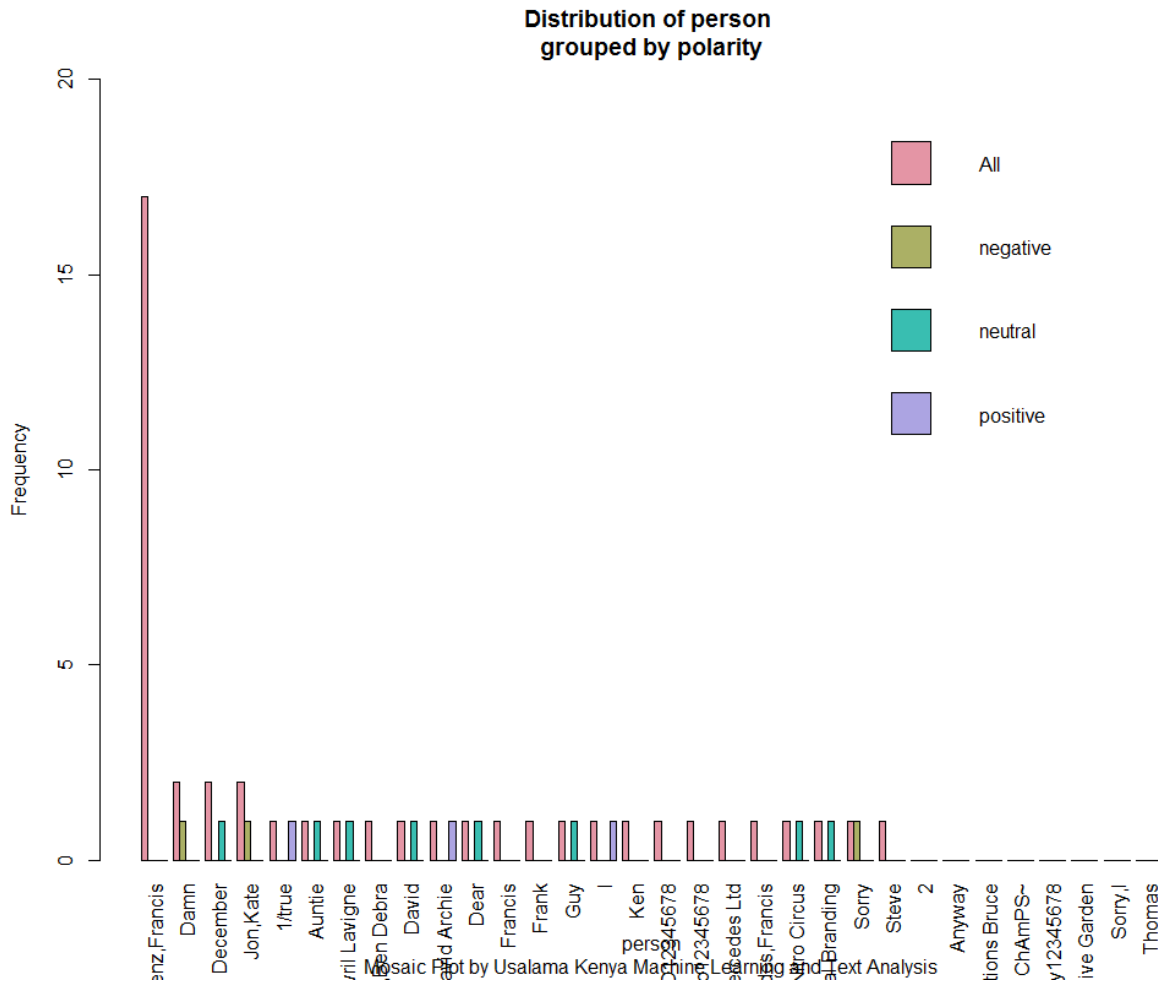
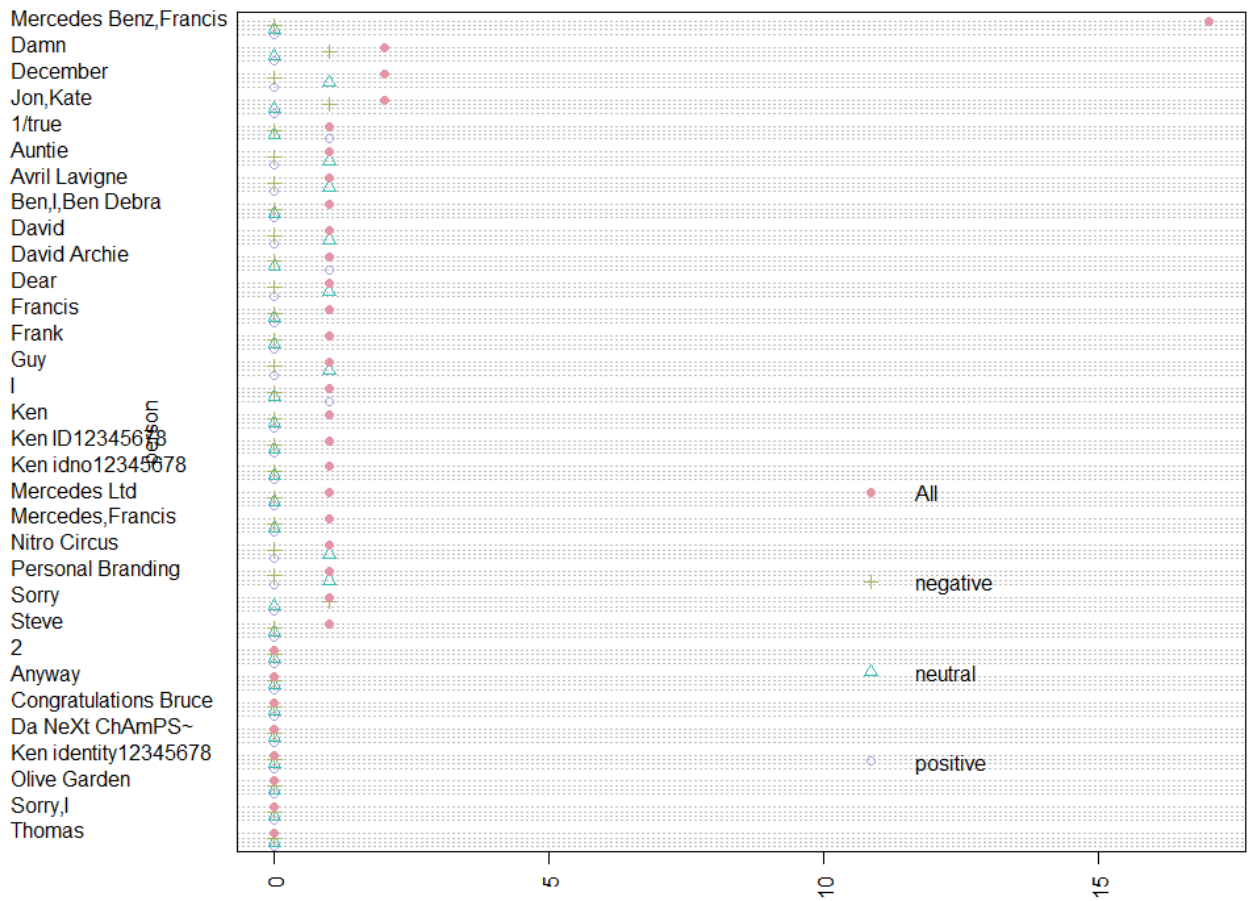


Figure 4-16: A Bar plot illustration of the distribution of persons by sentiment polarity

Distribution of person by polarity



Frequency
Dot Plot by Usalama Kenya Machine Learning and Text Analysis

Figure 4-17: A Dot plot illustration of the distribution of persons by sentiment polarity

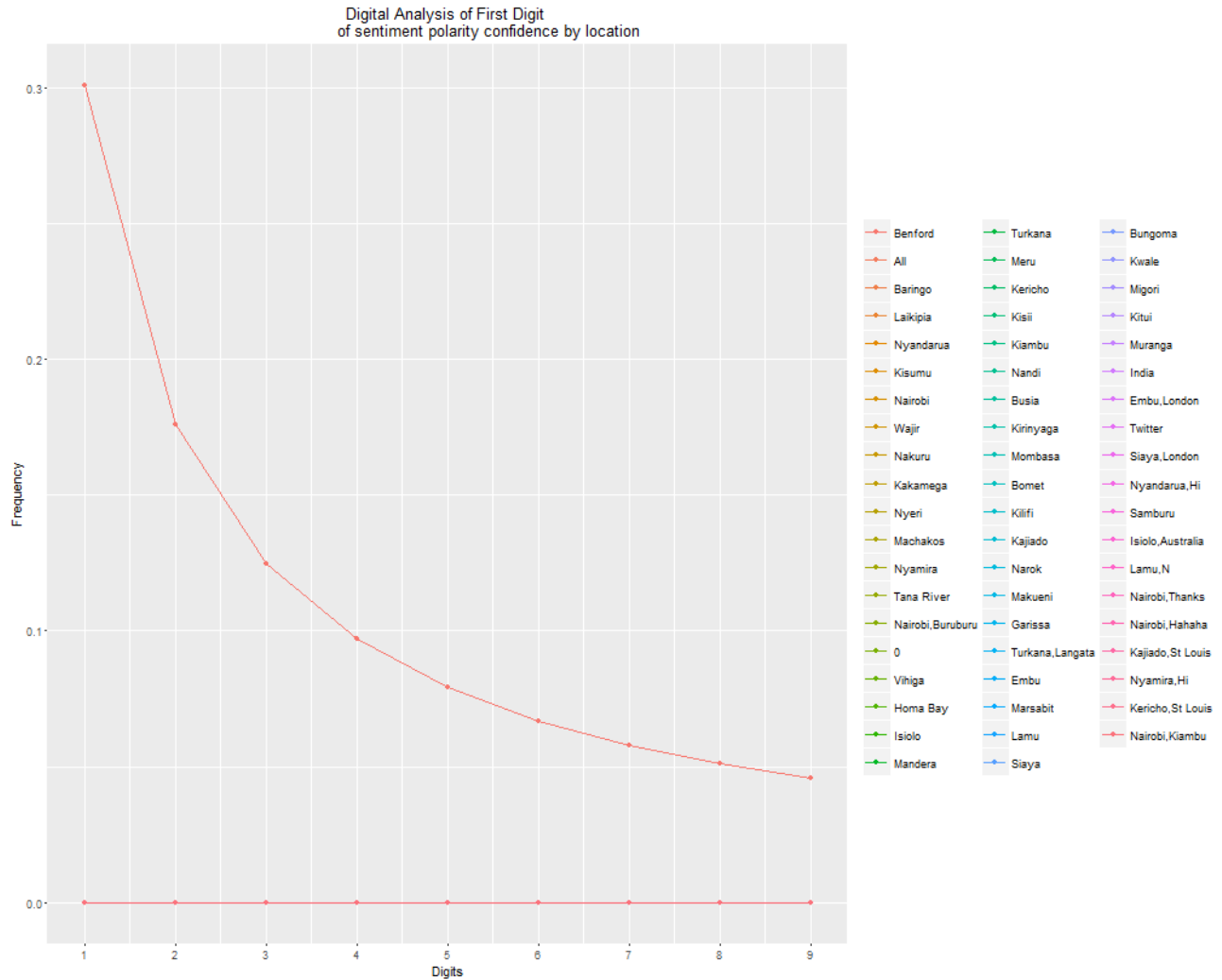


Figure 4-18: A Bedford's law digital analysis illustration of the distribution of persons by sentiment polarity

4.7.3 Distribution of Organisations

During the text mining analysis information, organisations' data was mined from the information that was submitted by the users via the mobile application. This data is later visually represented into various plots and charts in the web application for quicker understanding of the data.

The Figure 4.19 shows the bar plot of organisation versus the sentiment of the information that was submitted via the mobile application. This data has the frequency of the organisation name, together with the average sentiment polarity of the organisation as per the context of reporting that includes the levels of positive, neutral and negative. This makes every reported organisation

information have four-bar group per person. From the illustration, the messages that mentioned the organisation ‘TransNzoia’ were reported the most, whereas the ones pertaining to person ‘ABC’ and ‘JFK’ had the most distress than other organisations. The Figure 4.20 and Figure 4.21 illustrates the dot plot and histogram plot respectively for the same data explained above

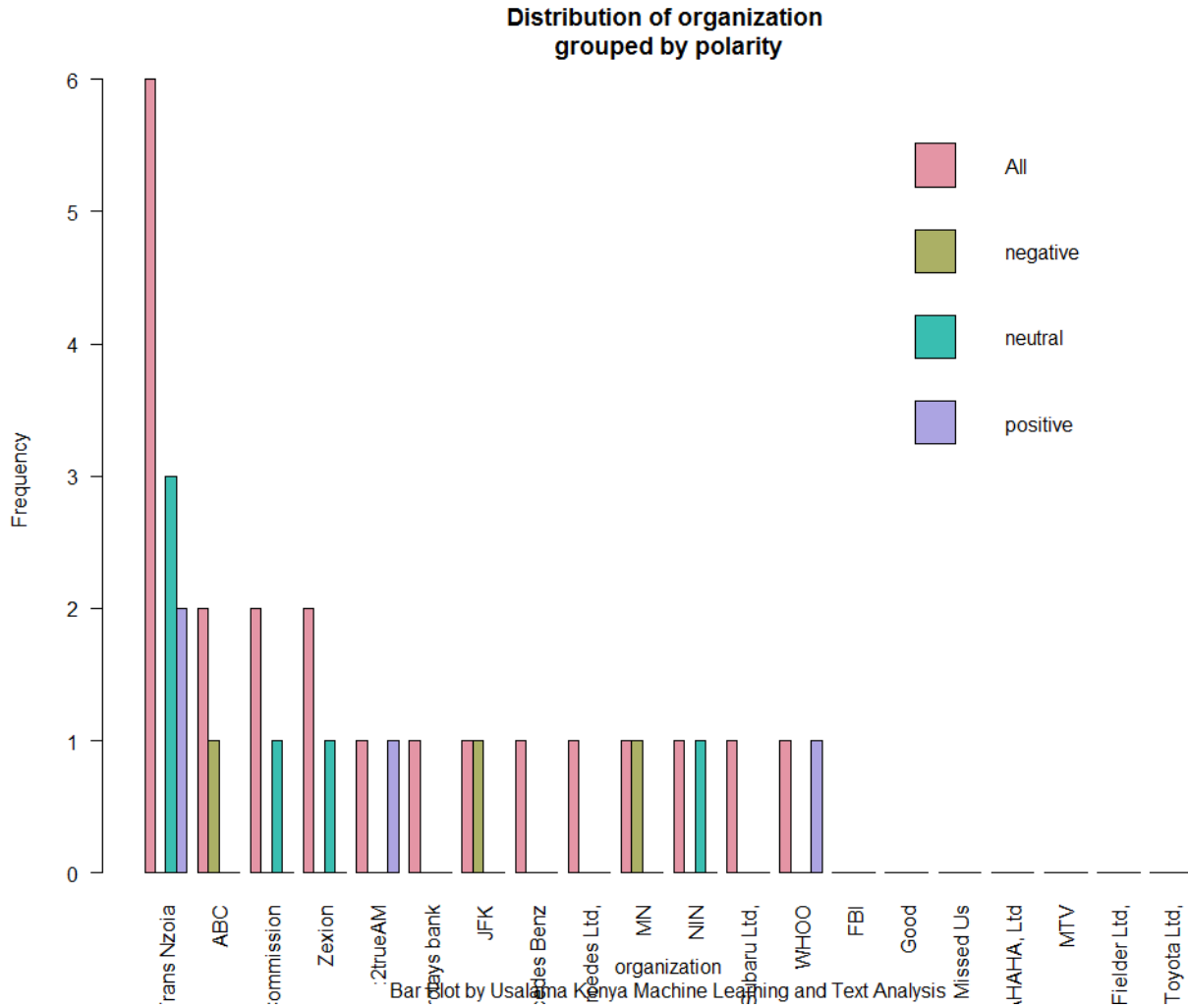


Figure 4-19: A Bar plot illustration of the distribution of organisations by sentiment polarity

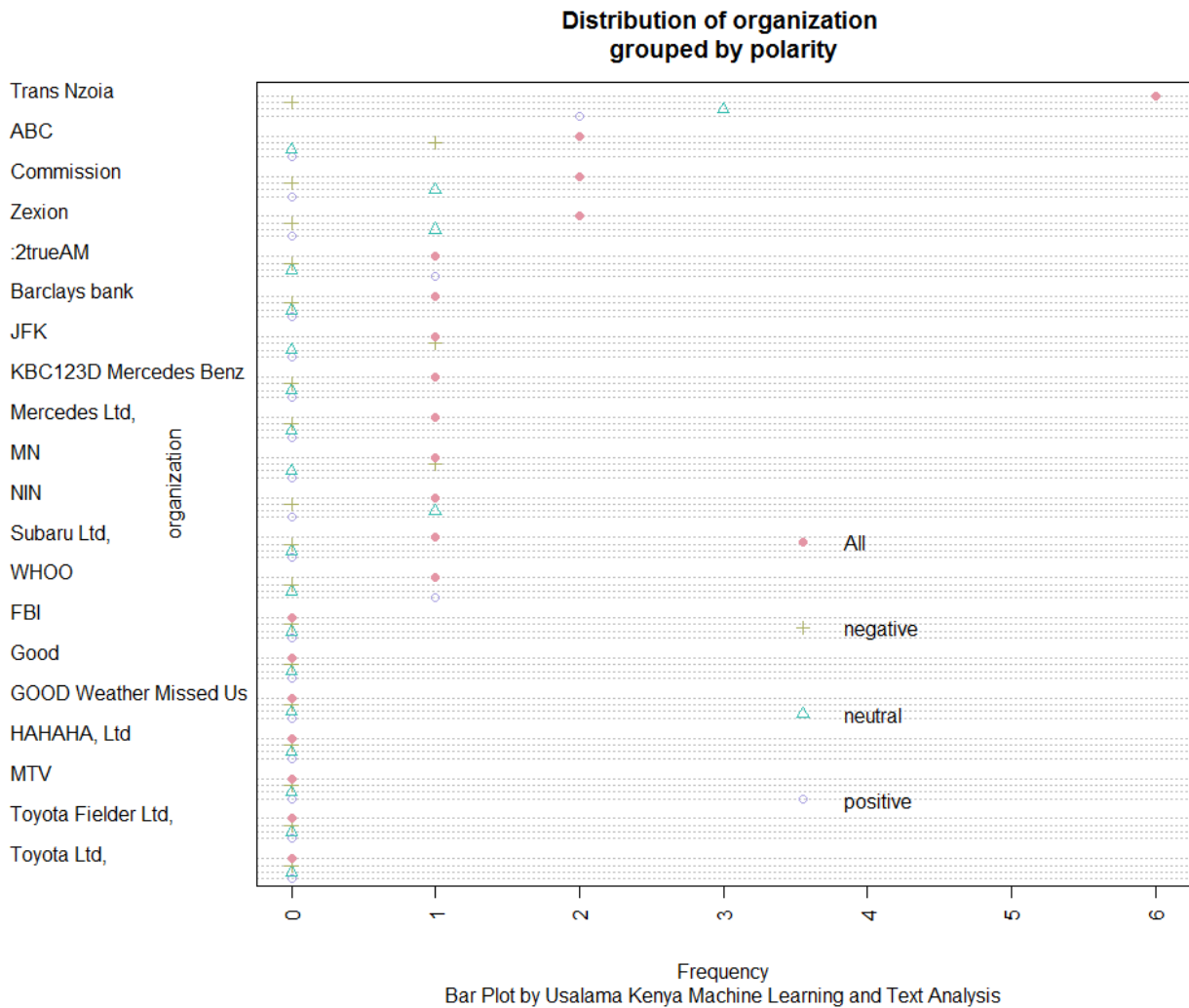


Figure 4-20: A Dot plot illustration of the distribution of organisations by sentiment polarity

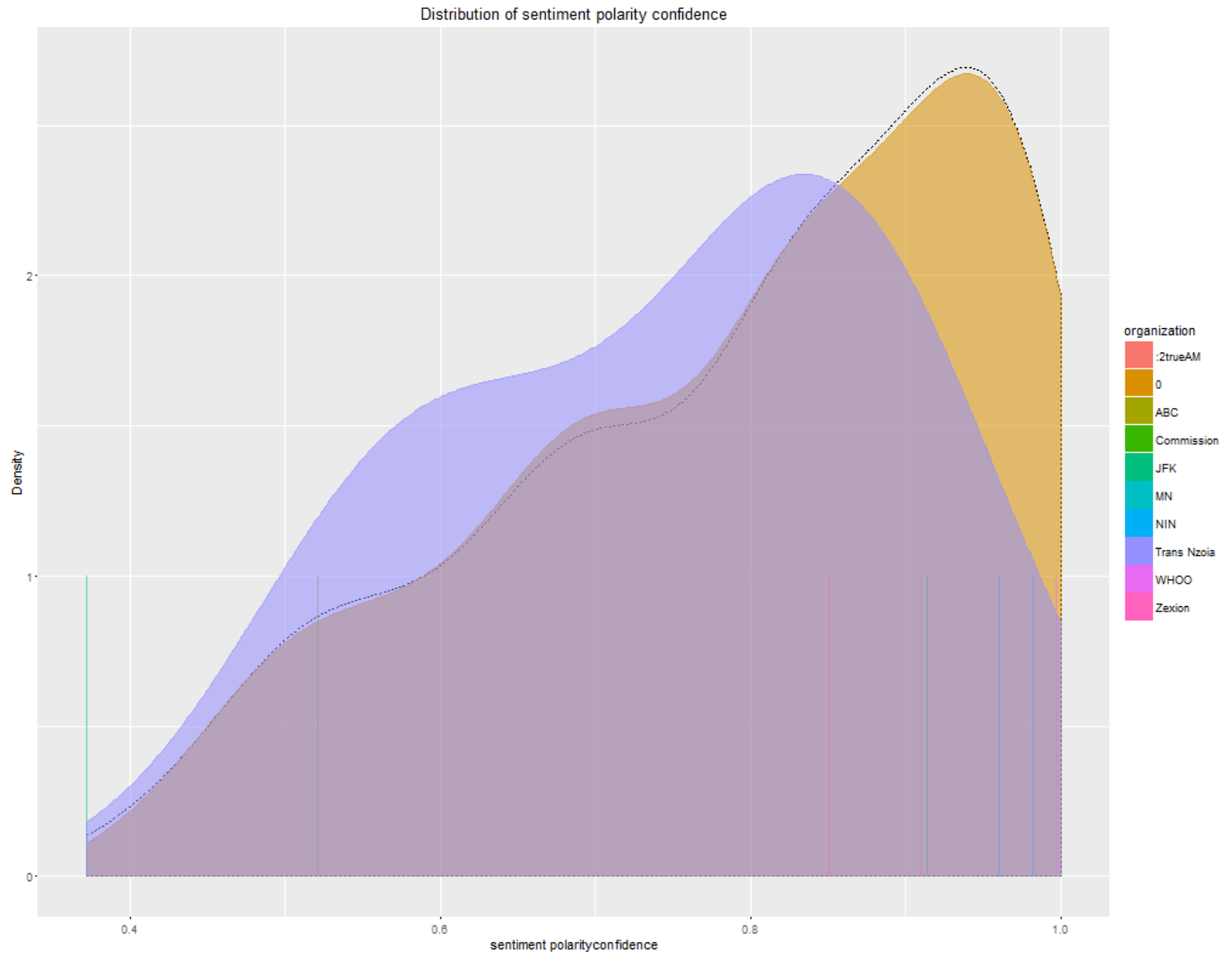


Figure 4-21: A Histogram illustration of the distribution of organisations by sentiment polarity

4.7.4 Distribution of Websites and URLs

During the text mining analysis information, website and URL data was mined from the information that was submitted by the users via the mobile application. This data is later visually represented into various plots and charts in the web application for quicker understanding of the data.

The Figure 4.22 shows the bar plot of websites and URLs versus the sentiment of the information that was submitted via the mobile application. This data has the frequency of the website and URLs, together with the average sentiment polarity of the websites and URLs as per the context of reporting that includes the levels of positive, neutral and negative. This makes

every reported website and URL information have four-bar group per website or URL. From the illustration, the first three URLs were reported the most, and none of them were mentioned in a negative sentiment context. The Figure 4.23 illustrates the dot plot for the same data explained above

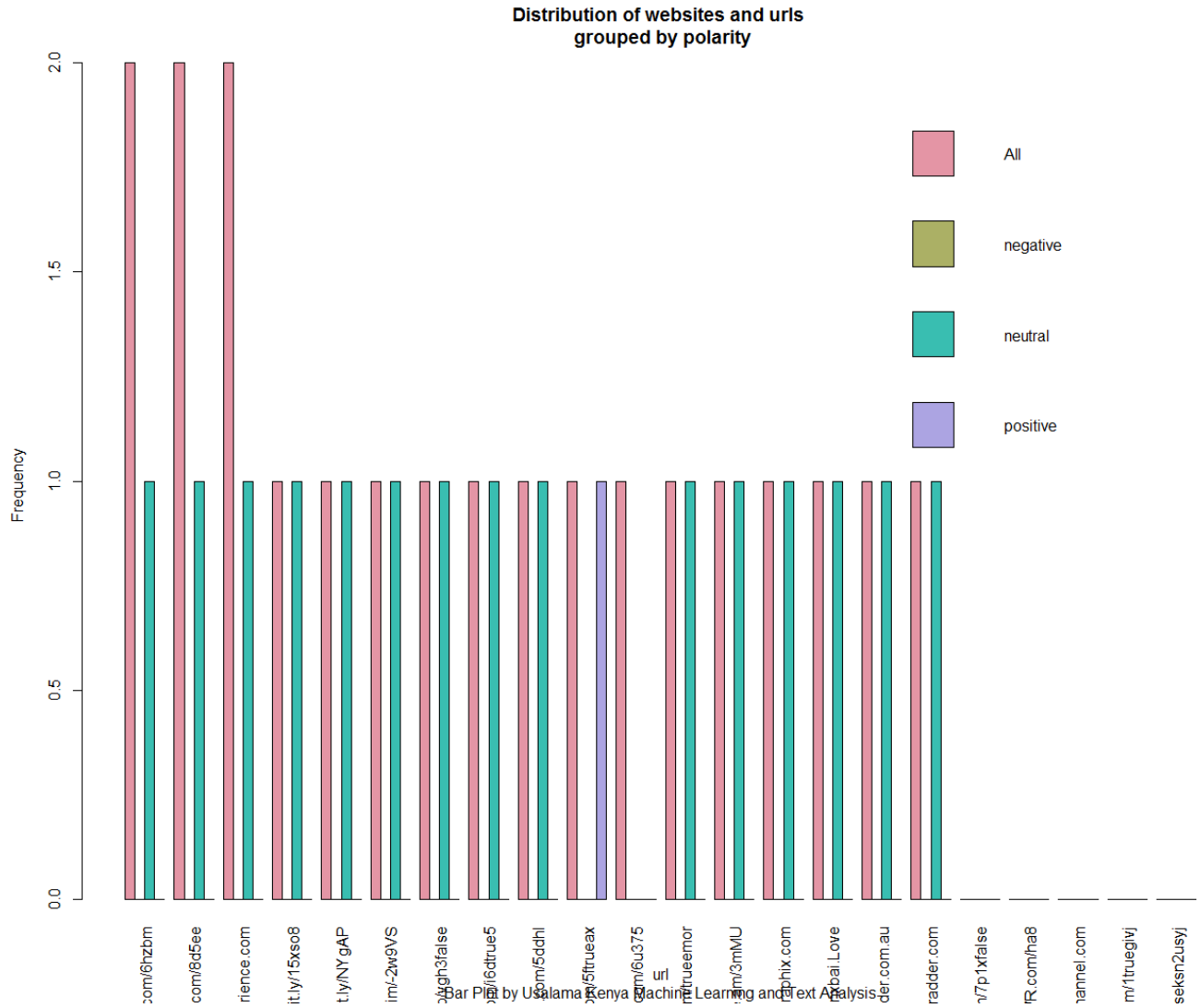


Figure 4-22 A Bar plot illustration of the distribution of websites by sentiment polarity

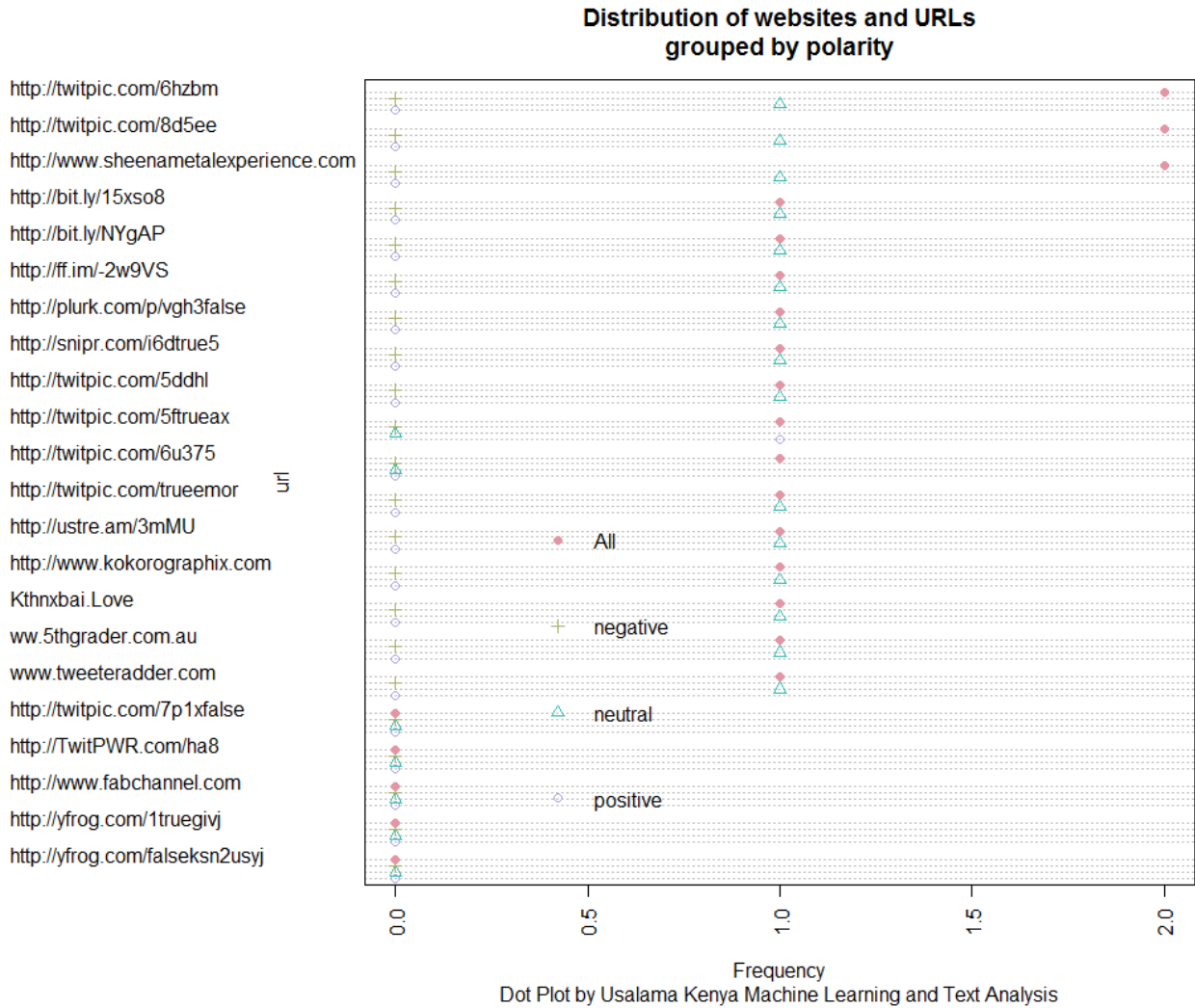


Figure 4-23: A Dot plot illustration of the distribution of websites by sentiment polarity

4.7.5 Distribution of Keywords

During the text mining analysis information, keywords were mined from the information that was submitted by the users via the mobile application. This data is later visually represented into various plots and charts in the web application for quicker understanding of the data.

The Figure 4.24 shows the most occurring term in all the hundreds of messages that have been submitted. Most commonly occurring are dates, followed by car models, counties and then people’s names, whereas figure 4.25 illustrates these terms in form of a word cloud.

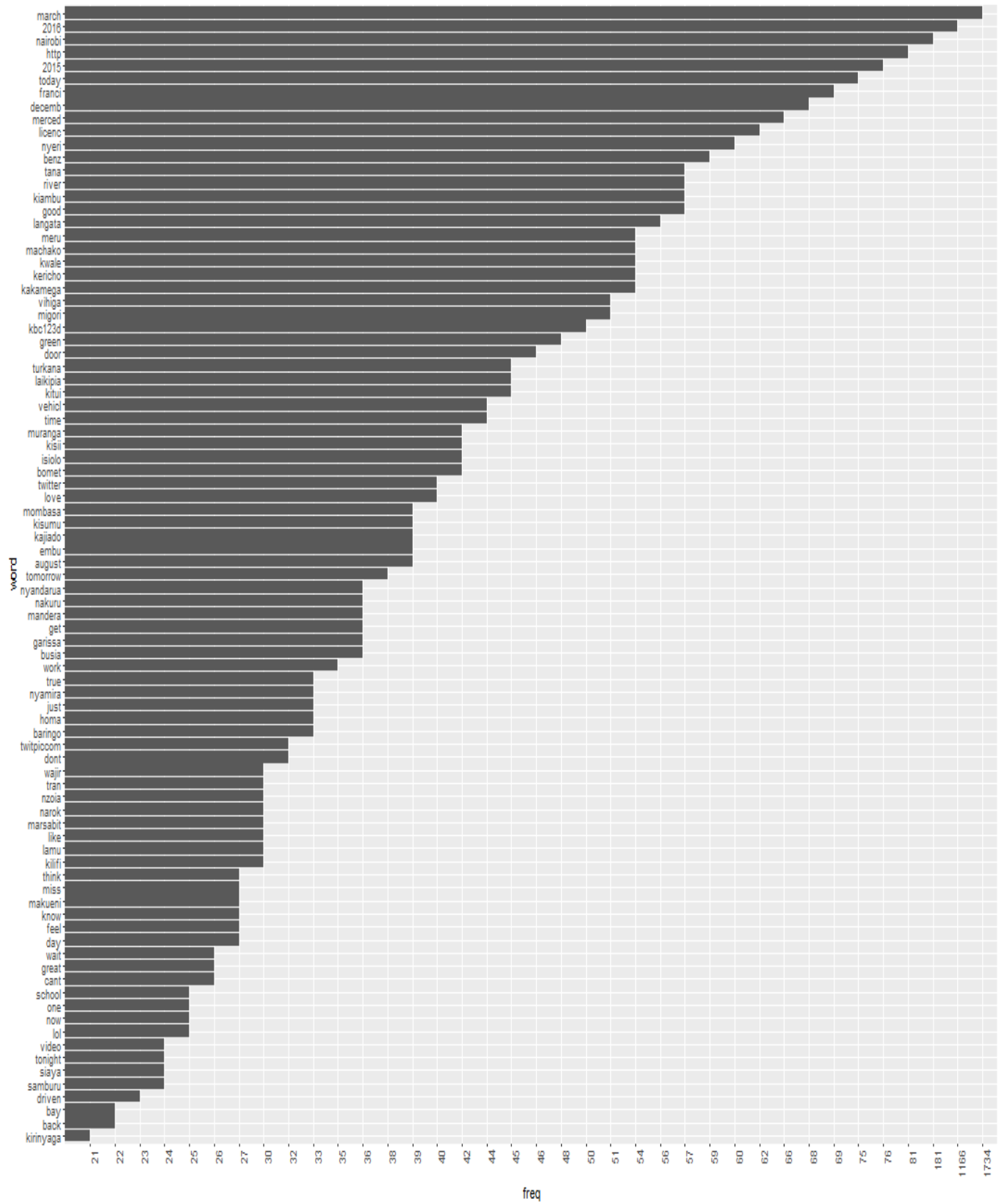


Figure 4-24: The most frequent keywords

4.8 Development

The system comprises of four major components, the mobile application, the web application portal and the machine learning system.

4.8.1 The Mobile Application

The mobile application is the component of the system that is used by the general public. Has been developed using the Android platform. The user submits the suspicious reports using the mobile application and this information is sent to the web based component.

4.8.2 The Web Application

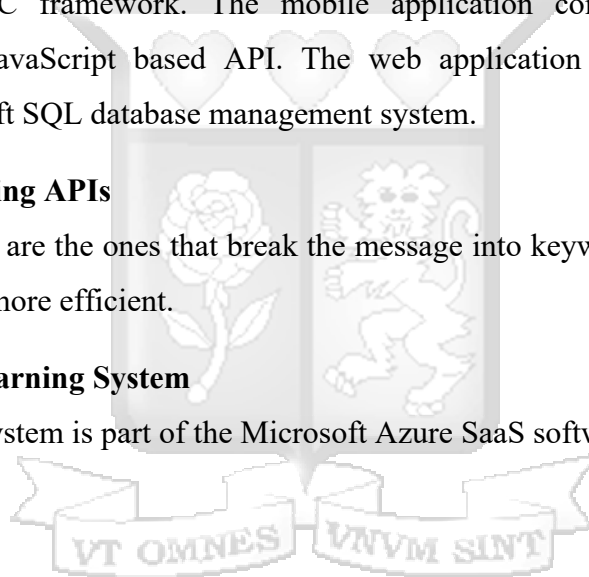
The web application has been developed using the PHP programming language, implemented using the Laravel MVC framework. The mobile application communicates to the web application through a JavaScript based API. The web application stores and retrieves the information in a Microsoft SQL database management system.

4.8.3 The Pre-Processing APIs

The Pre-Processing APIs are the ones that break the message into keywords and categorical data to make the text mining more efficient.

4.8.4 The Machine Learning System

The Machine Learning system is part of the Microsoft Azure SaaS software suite.



Chapter 5 : System Implementation and Testing

5.1 Introduction

5.2 Client Side System

The client side system is a mobile application implemented in the Android platform. This mobile application can be found on the Android Play Store, titled “*Usalama Kenya*”. The search result of this application is attached on Appendix D of this document.

5.2.1 Android Versions Support

The mobile application supports a minimal Android API version 11, which encompasses only up to Android version number 3.0 Gingerbread. The targeted API version is version 23, and also the maximum supported version, is Android version number 6.0. The build tools version used was 22.0.1.

5.2.2 Android Libraries

Despite the default Android Platform. Some additional libraries were used to achieve the goal of the system. These additional libraries are as follows.

a. Azure Mobile Services

This is the main library that interfaces with the secure mobile API endpoints in the cloud servers. It provides encryption by the use of an API key that the mobile clients should authenticate themselves to the server.

b. Google Cloud Messaging

This library is used together with the Azure Mobile Services libraries to provide push notifications to the users. The push notifications contains alerts, and news content that are initiated from the administration portal. A screenshot showing how a push notification from the administration portal is received in the mobile application is illustrated in appendix C.

c. Google Analytics

This library is useful when the administration needs to keep track of the mobile application usage, which phone models are mainly accessing the application and the geographical locations most users are in. This in turn creates reports on usage on the administration portal as shown below.

Figure 5.1 shows how the mobile application usage coming from the analytics library

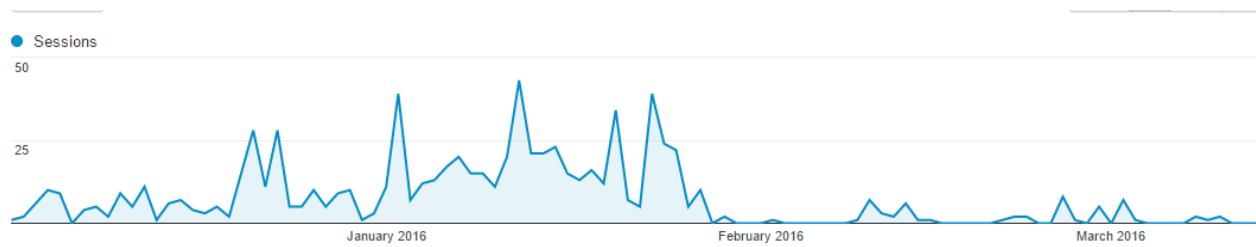


Figure 5-1: The mobile application usage

d. Google Play Service Ads

This library comes to play when an advertisement strip was added on the bottom of the news feeds and alerts activity in the mobile application. The advertisement was configured from Admob, the advertisement vendor, to display only content related to security awareness. A sample of the advert that has been implemented can be illustrated in the news feeds and alerts page of the mobile application in appendix C.

e. Google Play App Invite

This library is was added to the application to implement the mobile app sharing capability to grow the network. It enables the mobile application to send a Google Play Store link to invited users. The link can be sent via SMS or Email. These are obtained from the users phone and address book in their phones, by the use of a list.

5.2.3 Mobile Application Communication Endpoints

The mobile application communicates with two separate endpoints; both the Azure Mobile Services endpoint and the Cloudinary Image CDN endpoint.

a. Azure Mobile Services Endpoint

The mobile application first validates the inputs by the user then compiles the data into a data model that has been specified. Each form has its own data model that expects particular fields. It

is this data model that is bundled up by the Mobile Services library and encrypted using the API key and sent to the web services.

b. Cloudinary CDN Endpoint

Cloudinary is a Content Data Network, primarily for hosting multimedia. In this particular context, when the user of the mobile application chooses to capture a snapshot and submits, this image is compressed into the WebP image format and sent to this CDN. The link is accessed only via a HTTPS connection and an API key is provided to secure the initial context of the connection to these servers.

5.2.4 Input Validations

The mobile application, being of form nature, input validations were necessary to minimise the input error rates. The phone number fields were restricted to type number only. The counties field was made to be a drop down since the counties list is constant.

Some input fields were made mandatory while some were not. For instance, in the emergency form, the phone number is mandatory while the 'Other information' fields were not mandatory.

5.2.5 Application Components

The mobile application in the client side has four main components and four secondary components as described below.

a. Application Launch and Dashboard

This mobile application has a home page, which provides the user with four main options. A provision to navigate to the page where he can fill and submit information regarding suspicious persons, vehicles, events and locations or residences. A side menu is available to access other secondary functions of the application. These entail the help, about and exit menu options as well as a navigation option to go to the requests page. This is illustrated in the attached screenshots in appendix C.

The dashboard is an Android Activity that holds Android Fragments. The home page, as well as the Feeds, FAQ, about and the Share are Android Fragments. This implementation model was used to make the application user experience feel lighter and faster. The use of Android Activities on all these modules would have slowed down the application. The Emergency and Share buttons were placed on the home page for easier accessibility in relevance to their purpose. The emergency button is more effective being in the top of the page since if placed anywhere else it would easily be missed in the event of an emergency. The share button was placed at the top as well to encourage the users to share the application to more people. The four main icons in the home page were placed in a grid layout for better alignment and symmetry.

b. Reporting suspicious persons

There are various parameters through which one may report a suspicious person. These parameters include name, national identification number, phone number, and a general description. In case of a scenario where the user has more information regarding the suspicious person, there is an additional field for more information as well as a provision to take a snapshot of the particular person under suspicion. This is illustrated in the attached screenshots in appendix C.

There is a dropdown containing the counties from which the user is to select the county that is associated with the report. These counties are not being pulled from the database. Instead they are stored in the mobile application as an array.

The date of birth, despite being an optional field, is not a free input text. Instead a date picker was used to reduce the user input error rates and inconsistencies. These may include different date formats or just erroneous data.

The input fields are also customised depending on the type of input expected. The edit text that expects the person name performs an auto capitalisation on the first letter of every word typed in.

c. Reporting of suspicious vehicles

The user may submit information regarding a suspicious vehicle. The form has six fields: the county from where the car was last seen, registration plate number, the make of the vehicle, last seen location, the vehicle description and a provision to take a snapshot.

The edit text on the make of the vehicle has an auto complete feature, whereby it auto completes the vehicle manufactures name being typed in. The application has a list of the common vehicle manufactures names.

d. Reporting of suspicious locations

The user may submit information regarding a suspicious locations. The form has four fields: the county, the specific location of suspicion, a brief description of the suspicion. There is also a field for any additional information and a provision to take a snapshot. This is illustrated in the attached screenshots in appendix C.

e. Reporting of suspicious occurrences

The user may submit information regarding a suspicious occurrence. The form has four fields: the county, the specific location of suspicion, a brief description of the suspicion. There is also a field for any additional information and a provision to take a snapshot. This is illustrated in the attached screenshots in appendix C.

f. Reporting of emergencies

The user may submit matters that need urgent attention. The form has four fields: the county, the name of the person reporting, his/her phone number, a brief description of the emergency. There is also a field for any additional information and a provision to take a snapshot. This is illustrated in the attached screenshots in appendix C.

The emergencies form's fields are all mandatory. This was done for the purposes of collecting sufficient information of the reporter of the emergencies in case of a follow up call from the system administrator.

g. News feeds and alerts

The user may view the alerts and news feeds that have been sent from the administration portal. The news feeds contain a thumbnail, a title, the message content and the time it was posted. This is also coupled with the news viewer page to view the alert in full. This is illustrated in the attached screenshots in appendix C. The news alerts can both be accessed by launching the mobile applications from the applications menu and by tapping on the received push notification from the notification bar.

All the alerts are pulled from the database on launch, and are automatically updated on receiving a push notification. This page was implemented as an Android Fragment instead of an Android activity so that it can easily open when it is being launched by tapping on the received push notification from the phones notification bar. The alerts list not being a default Android list view, a customised list view was implemented, to accommodate the thumbnail image and the Android Relative Layout, which holds the strategically placed components per list row.

h. Application Share

The user may share the application to other users who exist in his/ her address book or phone book. The first time accessing this module, the mobile application prompts the user to select an already existing Gmail address in the phone's Gmail accounts. The user shall search, select and send invite. When the user invites, the mobile application shall send a deep link via SMS or email to these users. This is illustrated in the attached screenshots in appendix C. The deep link is a Google Play store link to download the mobile application. The sender address of this email shall be the email that was earlier specified by the user and as for the SMS, the SMS charges apply. A copy of an email that is received from the invite is attached in Appendix D.

This App Invite page contains the Cursor Adapter that picks the Address book items to display to the user. The application icon is not locally stored in the mobile application, instead it is cloud hosted. This is because the campaign icon can change from time to time while sharing the application to other users, subject to changing by the system administrator.

i. Sign Up and Sign In

The user may register to use the application using email address, telephone number and a password. It is with this information that the user shall log in to the application. An illustration of how the user shall be able to log in is illustrated in Appendix B.

j. Alerts via Map

The user may view the alerts regarding the surrounding areas that they are currently in, by the use of GPS. The user can see their current location on the map and if any threat has been reported in their area, it is shown in the map, in relevance to their current location. These threats

are shown by map markers with a description of the threat. On clicking the marker, more information is available to the user, along with a provision to share this information to other users.

These may be family members or friends who may be affected by the threat. The sharing of this information may be by the SMS, Whatsapp, Email, Twitter or Email. An illustration of how the user shall see the alerts is illustrated in Appendix B.

5.3 Web Services and Middleware

The web services of this architecture acts as the middleware between various components. These include the mobile application end, the third party library integration, the database layer and the administration portal. These are elaborated as below.

5.3.1 Integration with mobile application

The web services that interact with the mobile application consists of Node JS endpoints that expect POST data via the mobile services libraries integrated into the mobile application. The data is received as a data object. The data is extracted from this object and http validations are done against any possible injections. Upon successful validation, this data is then stored in the relevant tables in the database via an abstract data model that the Azure SaaS provides. After successful saving of the data. The pre-processing starts.

5.3.2 Integration with third party analytics APIs

Upon successful saving of this information, this data is subjected to a third party API for data pre-processing and text segmentation. The information that has been submitted from the mobile application is merged into one large text and is subjected into this API which then segments the text into particular categories. These categories are organisation, locations, persons, keywords, date, money, percentage, time, URL, email, sentiment polarity and confidence of sentiment polarity. These categories are then placed in a NoSQL schema, together with the original message in another database management system, awaiting further text mining and analysis.

5.3.3 Integration with database management infrastructure.

This middleware saves both the data from the mobile application as elaborated earlier as well as data that has been pre-processed. The former is stored directly to the Microsoft SQL server database, which is cloud hosted, and is accessed abstractly from this middleware. Whereas the latter is stored in a NoSQL table storage, and is accessed by providing the URL, and

authentication credentials. This database separation is because data stored in NoSQL is easier, faster and more efficient to access as Big Data as compared to data stored in the traditional relational database management system.

5.4 Server Side Web Administration Application

The server side application is a web based system that gives access to the system manager and other administrators, to view the information that users have submitted. A screenshot attached in appendix C shows the information about thousands of suspicious places that has been logged in the system.

5.4.1 Web Application Environment

The web application is being hosted on an IIS server in the Microsoft Azure platform. It is running on PHP version 5.6. This application was developed with the Laravel PHP framework and the visual representation of data as bar, line and pie charts is by amCharts.

The environment used a Dot Net Framework of version 4.6, to support the IIS server and neither Java nor Python support was added to the environment. Two domain names were mapped to this web application by the use of the IP address found on the domains **A Record**. The two addresses are vigil.azurewebsites.net and www.usalamakenya.com. The former was provided by the Azure platform whereas the latter is a purchased domain of preference.

The deployment was done by the use of Git, and as a result a Git deployment URL is provided, to access the web based command line terminal and web based file explorer for production environment customisations and management. The Git branch that the deployment is made is the master branch.

Three levels of logging were implemented. The web server logging which is provided by the IIS server, the application level logging which is implemented by PHP and database level logging, where any unexpected environment level exceptions are logged in a blob storage, provided by the Azure platform.

Virtual directories is implemented since the Laravel platform's web directory exists in the “./public” folder, and the *index.php* file found in the folder is that routes the traffic to the rest of the application. This was done to improve on web application security.

a. Web Application Deployment

The web application development and deployment took place in three phases. The first phase, both the web application and its database were created on a localhost. The second phase, the web application was connected on a cloud hosted database, while the web application itself being on localhost. The purpose of this was to allow the mobile application to pull some information from the cloud while the web application could obtain and analyse this data. The database was generated on the cloud environment by the use of database migration scripts. These scripts are triggered by the command “**php artisan migrate**”, on the web platform. A browser based command line prompt is provided by the Azure platform to allow the execution of scripts of this nature.

The third phase is the moving of the web application to the cloud hosted server. This was done through an integrated source control implementation, by use of Git. Git only moves the source files and not the dependencies. As a result, upon moving the source files to the server, the dependency packages were re integrated by use of Composer. Composer is a dependency management system for dependency based projects. Therefore, still on the web based command line console, the command “**php composer update**” is executed. This gets the dependencies to the project and updates any dependencies that might have been out dated. These dependencies include Sentry, used for authentication and authorization and Swift Mailer, for mail exchange server integration.

b. Web Application Integrations

The web application is integrated to both the database and the Azure Machine Learning platform. The integration of the cloud-hosted MS SQL Database is through the Eloquent ORM. For this integration to be successful, the URL of the database and the authentication credentials are configured in the web application to enable Eloquent ORM to interface to it. This web application does not interface with the NoSQL database directly.

Instead it interfaces with the NoSQL indirectly through the Machine learning platform, and this integration is made not to access the raw data, but the analysis plots and charts after text mining.

Integration with this platform is through a web service, which sends a JSON packed request and the response is JSON packed as well.

The analysis images are received as base64 images. Therefore, the images are first converted to PNG then displayed on HTML.

5.4.2 Application components

The server side has six main components. The suspicious people, vehicles, incidents and places logs, the dashboard with the charts and analysis and the reports.

a. Emergencies

All the emergency information that are submitted from the mobile applications are logged in this module

b. Information logs

This module contains four sub modules. It consist of the suspicious persons, vehicles, locations and places logs. The administrator can access this pages and view all the submitted information. These records are being fetched from the cloud hosted MS SQL relational database by the use of Eloquent ORM for efficiency.

c. Alerts

It is from this module that the administrator pushes the news feeds and alerts to all mobile application users. This module connects to the push notification module that has been implemented in the middleware web services. The push notification module first saves the alerts into the database then sends a push notification to all the users of this mobile applications. A screenshot attached in appendix C shows the alerts module in the web application.

d. Analysed Information

This module interfaces with the Azure Machine learning platform via a secure web service. It triggers the web service with request parameters and authentication token, which responds with the machine learning results. These results are not in picture format, neither PNG nor JPG. Instead, the response is a base64 representation of these images. These are converted on the fly as they get displayed in the web page. A screenshot attached in appendix C shows the graphical representation of the results.

5.4.3 Application security

The web based system is well secured and only administrators with the correct username and password can have access and must be on premise since it is restricted to a particular IP address range. The authentication and authorization of this web application was implemented by using the Sentry suite package. Sentry implementation issues a highly secure user administration and role management as well as a tokenised authentication. A screenshot attached in appendix C shows the login module in the web application.

5.5 System Testing

5.5.1 Mobile application testing

The android mobile application was tested for input validation when the user was expected to fill the suspicion forms across the four modules. Table 5.1 below illustrates the test case for a user creating a suspicious person report.

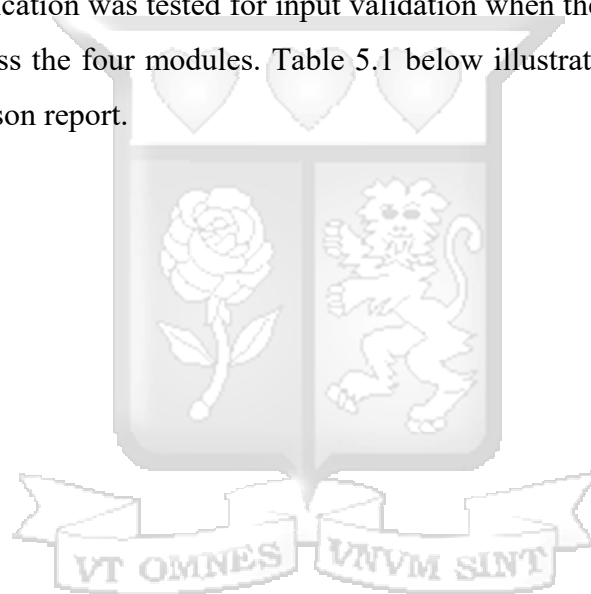


Table 5-1: Suspicious Person Submit Test Case

| | | | |
|--------------------------|---|--|------------------|
| Test Case Name: | Create suspicious person report | Test Case Number: | 1 |
| Brief Description | Test the action of filling in the form for reporting a suspicious person | | |
| Pre-conditions | The user has installed the mobile application into their phone and it is launched for the first time. | | |
| Step | Action | Expected Response | Pass/Fail |
| 1 | User taps the suspicious persons icon | User is taken to suspicious person form | Pass |
| 2 | The user may choose to leave blank all fields except the description field | A prompt when the user attempts to submit without the description field. | Pass |
| 3 | The taken snapshot should be visible only when user has captured an image | The image control is invisible unless the user takes a snapshot | Pass |
| 4 | User should get successful submission after they have submitted the form. | The application navigates to the dashboard page | Pass |
| Post Conditions: | Suspicious person details are saved in the database. | | |

5.5.2 Web application testing

The web application was tested thoroughly and the all the attention was focused on its security.

Table 5.2 below illustrates the test case which was conducted to ascertain sign in not to occur in through an IP address that had not been configured in the system.

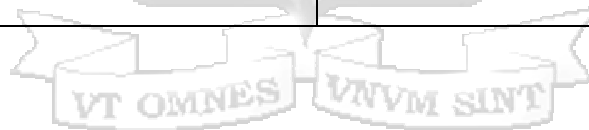
Table 5-2: IP Restricted Authentication Test Case

| | | | |
|--------------------------|---|---|------------------|
| Test Case Name: | IP Restricted Authentication | Test Case Number: | 2 |
| Brief Description | Test the action of not granting authentication to invalid IP address | | |
| Pre-conditions | The user is online and able to access the web browser | | |
| Step | Action | Expected Response | Pass/Fail |
| 1 | User enters credentials while laptop connected to a different LAN cable | System shows a prompt that the user is not authorized to login from that network. | Pass |
| 2 | Laptop connected to the in premise network and provides correct authentication details. | User is successfully logged in. | Pass |

Table 5.3 below illustrates the test case which was conducted to demonstrate how the system is capable of predicting a suspicious persons names

Table 5-3: Predict Suspicious Persons Name Test Case

| | | | |
|--------------------------|--|--|------------------|
| Test Case Name: | Predict Suspicious Persons name | Test Case Number: | 3 |
| Brief Description | Test the action of predicting the suspicious person's name based on other information provided | | |
| Pre-conditions | The system already has information that users have already submitted | | |
| Step | Action | Expected Response | Pass/Fail |
| 1 | User enters information that shall be used to predict the name | System displays a list of potential names and scores ranging between 0.0 and 1.0 | Pass |
| 2 | User enters no information and goes ahead to select the Predict menu button | System prompts the User to provide sufficient information to yield a better prediction | Pass |



Chapter 6 : Discussions of Results from the Testing

The purpose of this research was to determine the challenges experienced by Kenyan Citizens and Kenya Security Personnel in relation to reporting and analysing criminal activities and propose a mobile application that would assist in mitigating the challenges. The research clearly illustrates the technology used to develop the mobile application and it gives a detailed explanation on the steps followed. By examining current mobile applications developed for reporting and analysing criminal activities, the researcher was able to determine features that would be included in the development of this mobile application.

6.1 Review of Research Objectives in Relation to the Mobile Application

The research objectives stated in the research provided a guideline in the development of the mobile application.

The first objective was to identify the current advancements in technology used to capture information regarding criminal activities. This was achieved by going through technical reports, scholarly journals, literature review articles, reference books, official statistics, product websites and google play. The researcher was able to use work done by previous researchers to be able to analyse features in current system and apply missing features in the proposed solution.

The second objective was to determine the challenges experienced by the population in terms of reporting crime and analysing criminal activities. This objective was achieved through the use of document review which involved using technical reports and scholarly journals which provided in depth information of challenges people face when they want to report issues on criminal activities.

The third objective was to explore the current models and frameworks used to develop mobile applications. This objective was achieved in Chapter 2: Literature view which illustrates the as current models and frameworks used. The current models and frameworks identified provided a guideline in the selection of an appropriate framework for the design and development of the mobile application.

The fourth objective which was to design and develop a mobile application that can let users report crime and let the proper authorities draw analytical conclusion that can prevent the same

crime occurring again. This objective was achieved in Chapter 4: System Analysis and Design as a mobile application was developed on the android platform and was implemented.

The fifth objective was to perform the required system testing on the mobile application. This objective was achieved in Chapter 5: System Implementation and Testing by performing testing on the mobile application and checking for any errors and bugs in the system. Test cases were used to indicate that the system modules passed all their test criteria and there was no error in the final system.

6.2 Review of the Proposed System

The proposed system is an android based solution that allows users to make reports on suspicious vehicles, suspicious persons, suspicious incidences, suspicious, submission of emergencies and responds to the requests that the security administration posts to the application for more information. The application has an administrative web-based backend that lets the users to receive the logs submitted by the users in the mobile application and it connects to the Azure Machine Learning platform to analyse the data and get more relationships regarding the different forms of information it receives.

6.2.1 Advantages of the Proposed System

The advantages of the proposed system include the following:

- i. Uses machine learning to perform analytic conclusions
- ii. Has an aspect of artificial intelligence which provides the security personnel with data regarding criminal activities.
- iii. The proposed system provides users with a portal to report criminal activities

6.2.2 Limitations of the Proposed System

The limitations of the proposed system include the following:

- i. The mobile application requires an android device that can access Internet connectivity.

6.3 Summary

The highlighted advantages show that the mobile application is an efficient system that can be used to monitor crime and prevent regular criminal activities taking place in the same location. The mobile application can help curb out insecurity within Nairobi County.



Chapter 7 : Conclusions and Recommendations

7.1 Conclusions

The research determined the challenges encountered by security personnel when it comes to analysing reports made by citizens with regards to criminal activities. The challenges include lack of establishing a pattern in certain crimes that take place in certain areas, lack of knowledge of the proper protocol of reporting criminal activities, lack of a mobile platform for reporting criminal activities and providing reports that can lead to conclusive information to establish criminal patterns.

In light of these challenges, a mobile and web based application was developed. The application was developed with the aim of mitigation against the challenges determined from the research. The outcome of the system evaluation and testing showed that the system enabled users to make detailed incident reports in addition to tracking their progress. It was also able to permit successful assignment of incident reports to relevant security personnel as well as provide a means to follow up on resulting actions. The developed system can be used to enhance the entire lifecycle of incident reporting from the initial step of making a report to the final step of resolving the incident and enumerating actions taken.

7.2 Recommendations

The research aimed to provide an efficient means for collecting and analysing information regarding criminal activities through the use of technologies such as GPS, maps, phone camera, machine learning and other web technologies. The solution would be a complete success if it was supported by the Kenyan government so as to encourage security personnel to use and also encourage citizens to use the application. The following recommendations are suggested:

- i. Development of National Database that can be used by the Kenyan government.
- ii. Providing a means of protecting identity of users who report criminal activities.
- iii. Designing more report formats to analyse the criminal activities posted by users.
- iv. Create awareness of the mobile application by use of social media and word of mouth.

7.3 Future Work

The proposed solution will facilitate the generation of detailed reports that with assistance in drawing conclusive information regarding crimes occurring in certain vicinities, as well as attaching a photo of the criminal activity. Future researchers can use this solution to include features such as video recording of the incidents.



References

- Aarabi, P. (2013). *tips for creating great mobile application user interfaces*. Retrieved February 28, 2015, from VB News: <http://venturebeat.com/2013/04/08/5-tips-for-creating-great-mobile-app-user-interfaces/>
- Adika, A. (2014). *Is Nyumba Kumi initiative destined to succeed in Nairobi?* Retrieved February 26, 2015, from Sauti ya mtaa: <http://www.sautiyamtaa.com/news-article/is-nyumba-kumi-initiative-destined-to-succeed-in-the-ghetto/>
- Agangiba, W. A., & Akotam, M. A. (2013). Mobile Solution for Metropolitan Crime Detection and Reporting. *Journal of Emerging Trends in Computing and Information Sciences*, 4(12).
- Aronson, S. L. (2013). Kenya and the Global War on Terror: Neglecting History and Geopolitics in Approaches to Counterterrorism. *African Journal of Criminology and Justice Studies*, 7(1 & 2). (2005). *Crime Analysis Defined*.
- Frilander, M., Lundine, J., Kutalek, D., & Likaka, L. (2014). *New technologies for improving old public security challenges in Nairobi*. IGARAPE Institute.
- Google. (2012). *CrimeReports.com encourages broad citizen participation in neighborhood crime prevention using Google Maps*. California, USA: Google.
- Herbling, D. (2012). *Police announce 7,000 vacancies ahead of elections*. Retrieved February 26, 2015, from Business Daily: <http://www.businessdailyafrica.com/Police-announce-7-000-vacancies-ahead-of-elections-/-/539546/1608514/-/uhp66mz/-/index.html>
- Schroeder, J. (2013). *Document Title: COPLINK: Database Integration and Access for a Law Enforcement Intranet, Final Report*.
- Kariuki, J. (2014). *Nyumba Kumi the surest way to enhance security in Kenya, says Joseph Kaguthi*. Retrieved February 26, 2015, from Daily Nation: <http://www.nation.co.ke/counties/nakuru/Joseph-Kaguthi-Nyumba-Kumi-/-/1183314/2495060/-/7sxp6z/-/index.html>
- Lee, V., Schneider, & Schell, R. (2010). *Mobile Applications/Architecture, Design and Development*.

- Mutahi, P. (2011). *(In)security, crime and gangs in Nairobi informal settlements*. Institute for Security Studies.
- Nilsson, E. G. (2008). *Design guidelines for mobile applications*. SINTEF.
- nola.gov. (2014). *Crimestoppers*. Retrieved February 27, 2015, from City of New Orleans: <http://www.nola.gov/nopd/citizen-services/crimestoppers/>
- Ogwueleka, F., & Ocheme, I. (2014). Review of RSA Algorithm Encryption for Combating Cybercrime: A Case Study of Developing Country. *International Journal of Emerging Technology and Advanced Engineering*, 4(9).
- Omanga, D. (2015). Chieftaincy' in the Social Media Space: Community Policing in a Twitter Convened Baraza. *International Journal of Security & Development*, 4(1).
- Omondi, S. (2013). *AN ASSESSMENT OF THE IMPACTS AND RECOMMENDATIONS OF PHASES ONE AND TWO OF CRIME PREVENTION TRAINING*. Nairobi: USIU.
- Otiono, J. (2013). *To Kenyans, police officers are the enemy within*. Retrieved Februar 26, 2015, from Standard Digital: http://www.standardmedia.co.ke/?articleID=2000094760&story_title=to-kenyans-police-officers-are-the-enemy-within
- Sitole, D. (2012). *Kenyan Chief Tweets His Way to Reducing Crime*. Retrieved February 26, 2015, from IPS: <http://www.ipsnews.net/2012/02/kenyan-chief-tweets-his-way-to-reducing-crime/>
- Sprunger, J. (2012). *Mobile Architecture Best Practices: Best Practices for Mobile Application Design and Development*. WestMonroe.
- Sun, E. (2014). *How mobile technology is being used to fight crime by police departments*. Retrieved February 26, 2015, from Quora: <http://www.quora.com/How-mobile-technology-is-being-used-to-fight-crime-by-police-departments>
- Cook,T. (2010). *What was the most popular mobile phone operating system in the world in 2010*. Retrieved February 27, 2015, from Distanceshores: <http://distantshores.org/blog/what-was-most-popular-mobile-phone-operating-system-world-2010>

Udemans, C. (2014). *67% of phones sold smartphones – Safaricom*. Retrieved February 26, 2015, from Human IPO: <http://www.humanipo.com/news/42985/kenyas-smartphone-penetration-at-67-safaricom/>



APPENDIX A: Other Result Findings

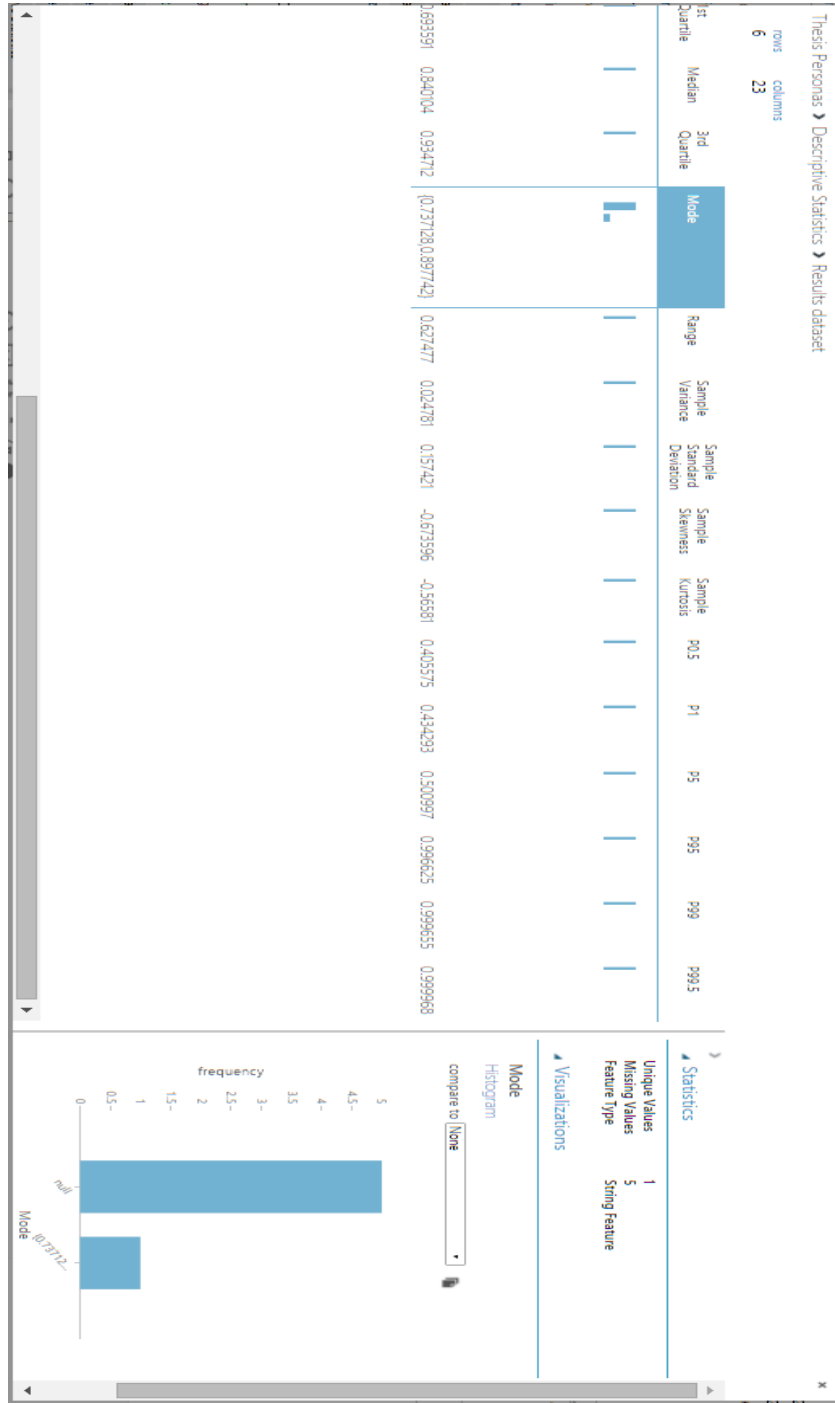


Figure A-1: The descriptive statistics of the original dataset

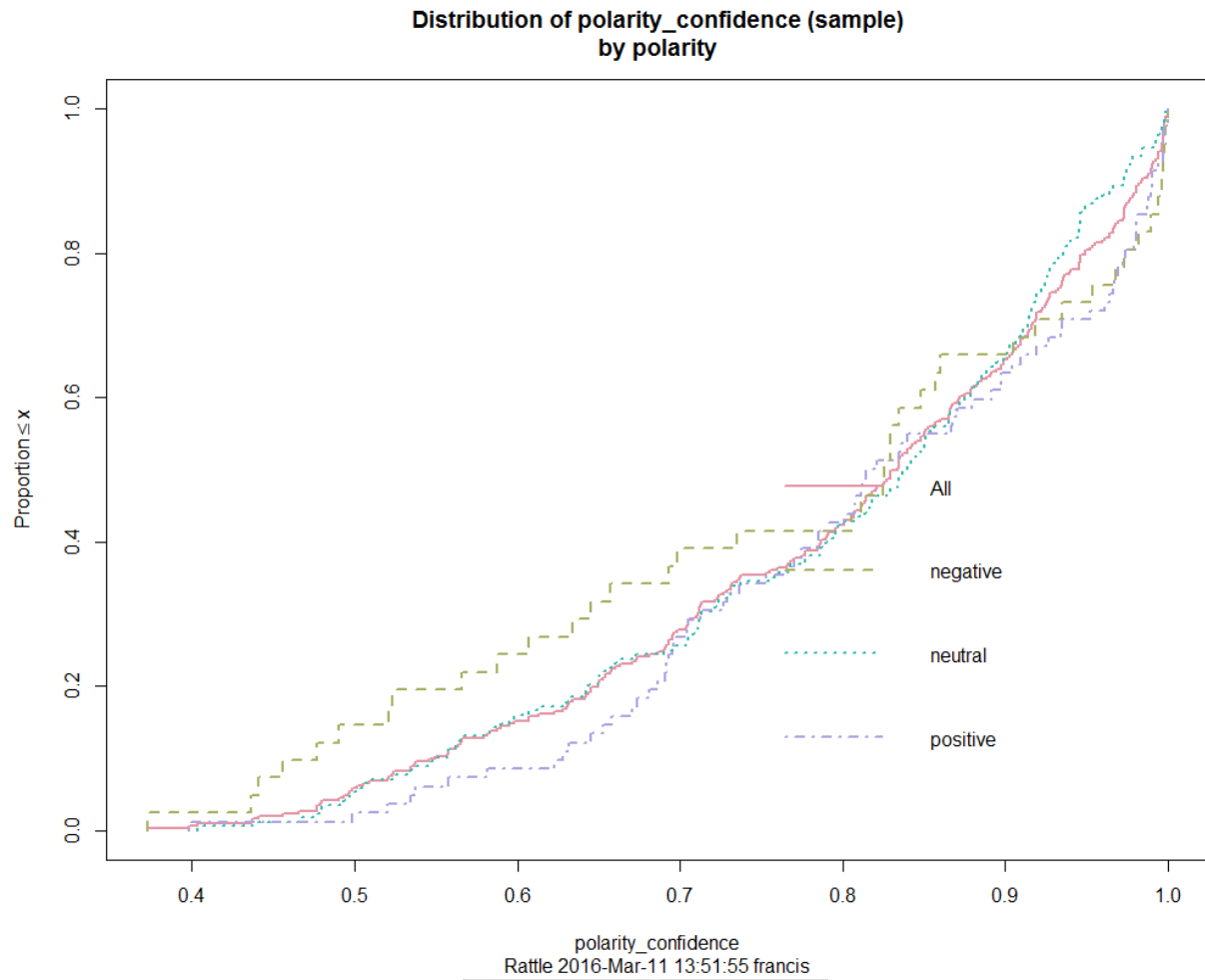


Figure A-2: A line graph of the distribution of sentiment polarity confidence by the polarity



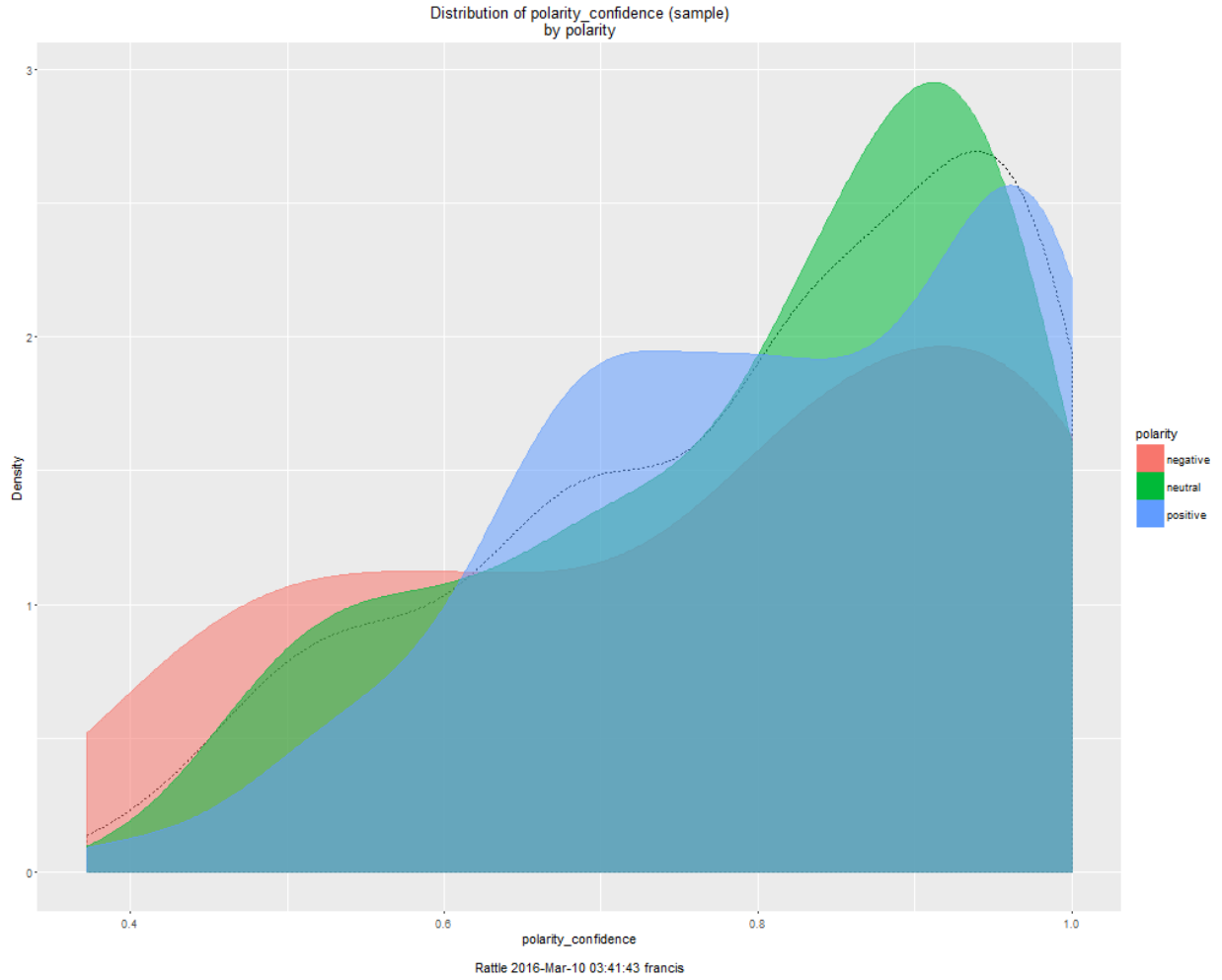


Figure A-3: A histogram of the distribution of sentiment polarity confidence by the polarity



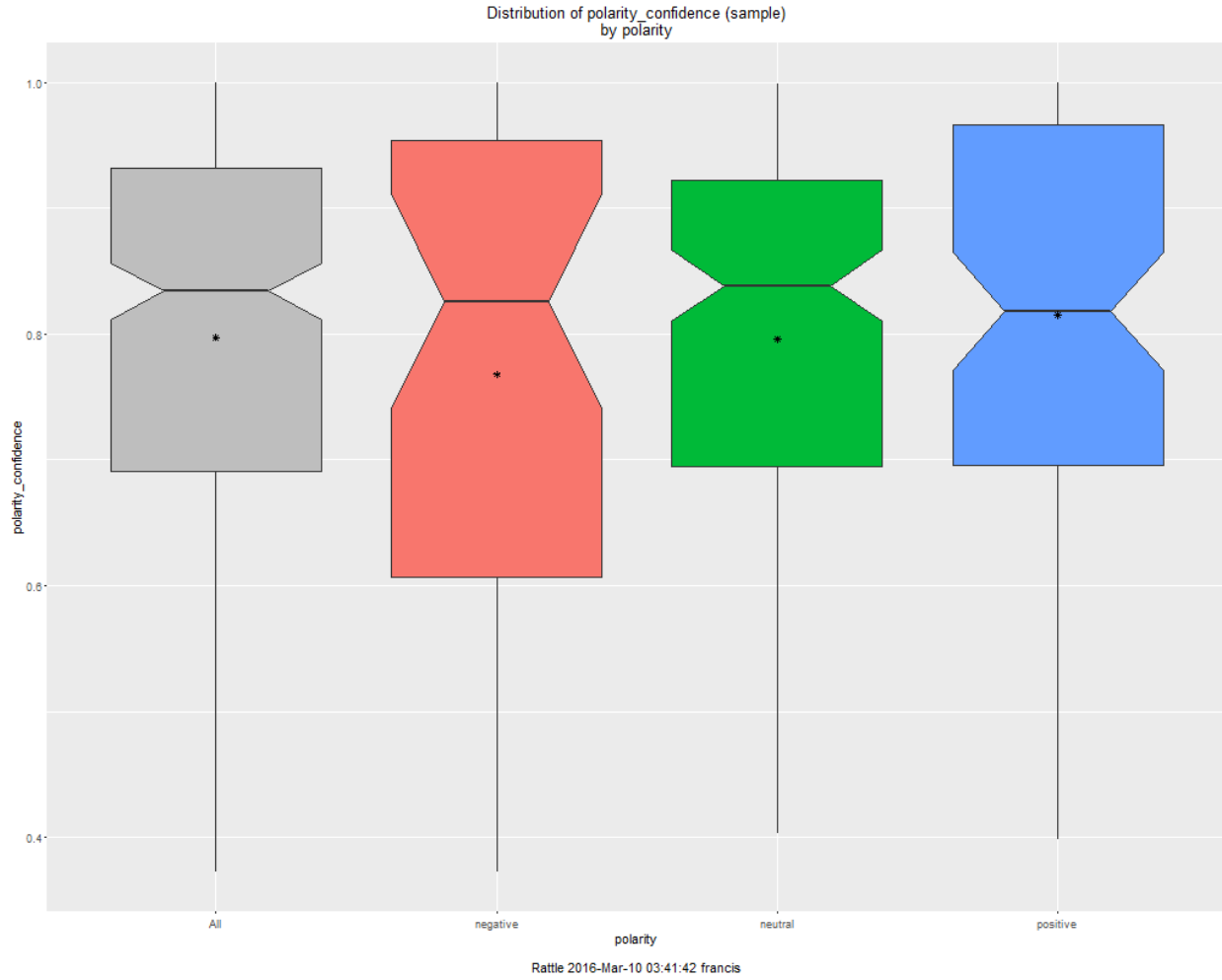


Figure A-4: A box plot of the distribution of sentiment polarity confidence by the polarity



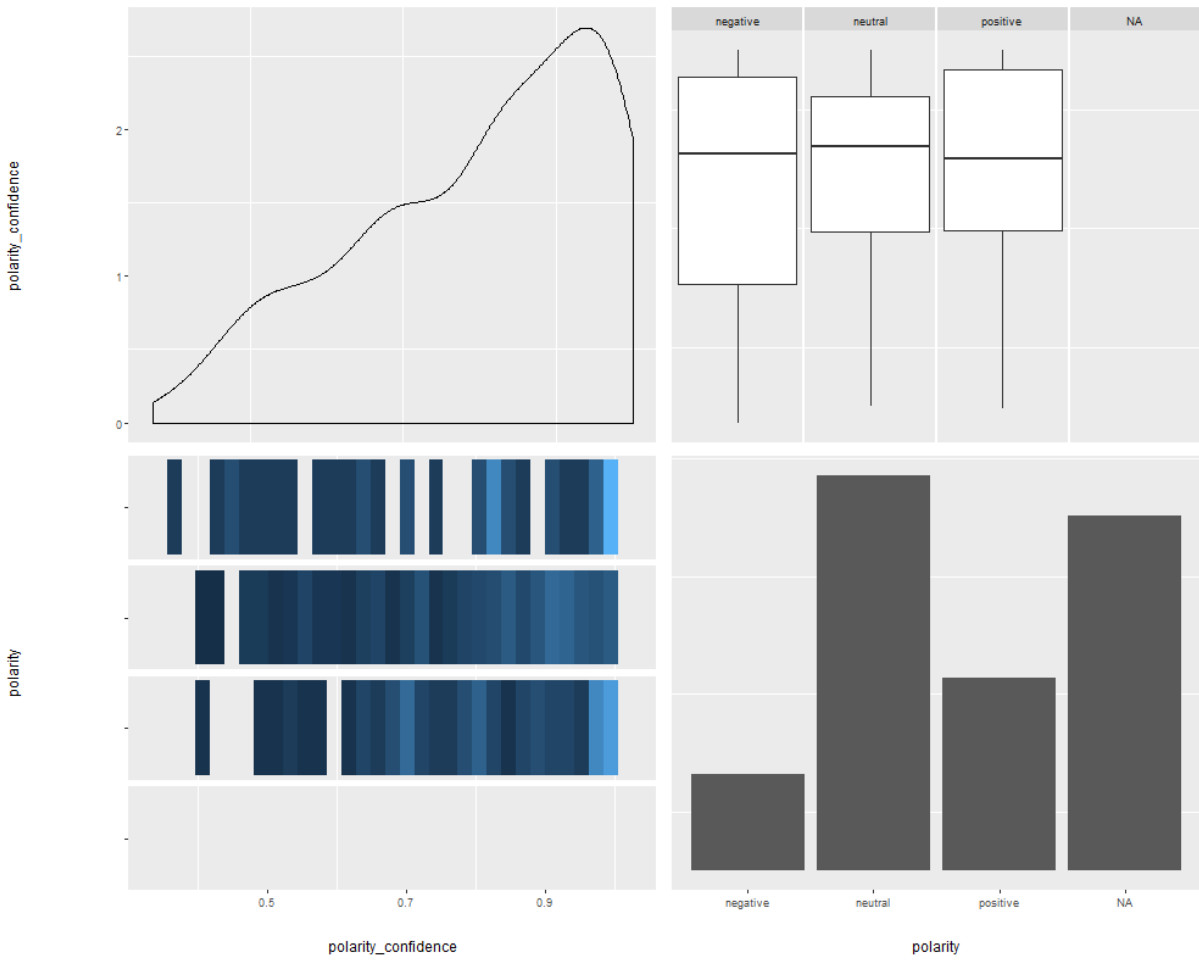


Figure A-5: A pair matrix distribution of the sentiment polarity confidence by the sentiment

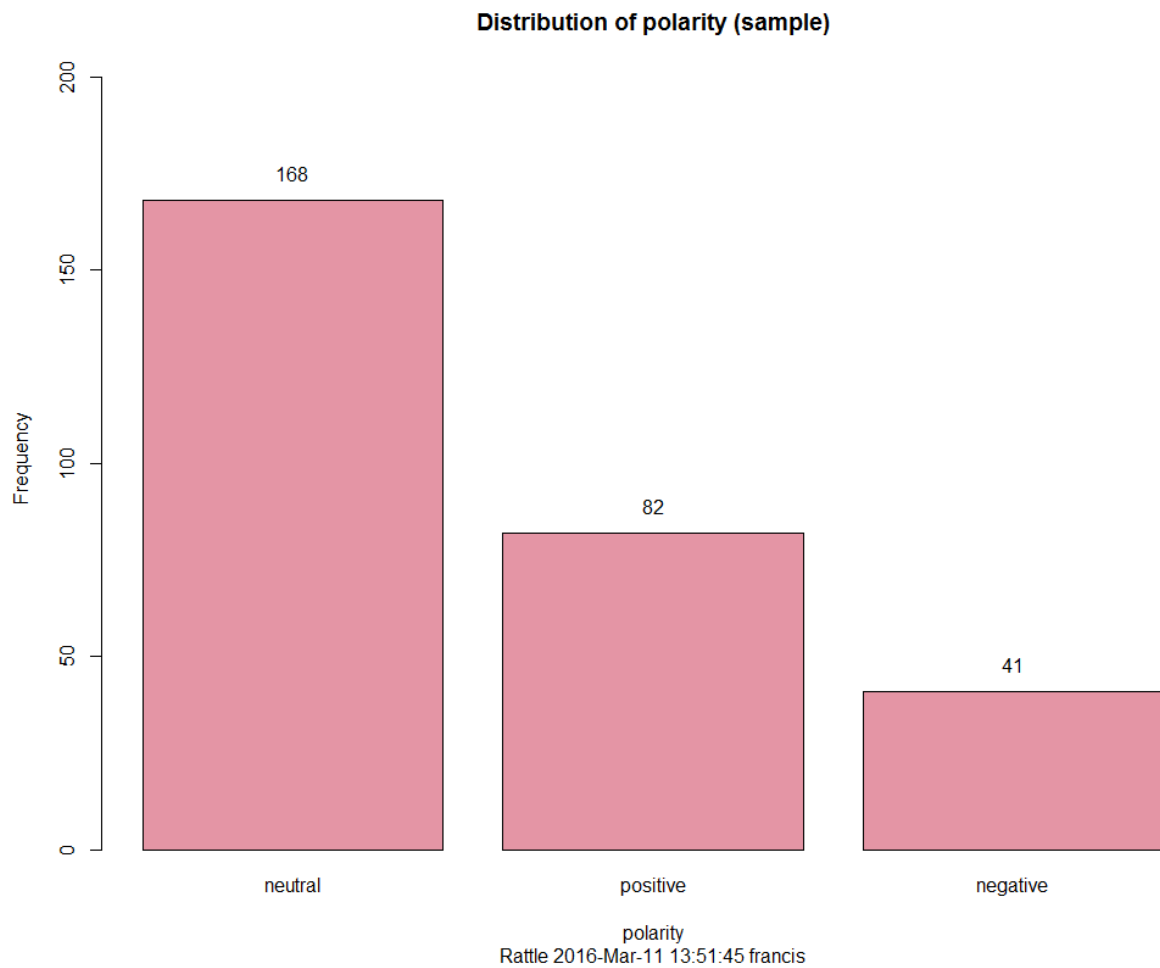


Figure A-5: A bar graph of the distribution of sentiment polarity confidence by polarity.



APPENDIX B: Turn it in Report

MSc IT Thesis 2014 Thesis Proposal - DUE 29-May-2015

Originality GradeMark PeerMark

A MOBILE AND CLOUD APPLICATION FOR INTELLIGENCE GATHERING: A CASE
BY FRANCIS OMONDI

turnitin 23% SIMILAR -- OUT OF 0

A MOBILE AND CLOUD APPLICATION FOR INTELLIGENCE GATHERING: A CASE
STUDY OF NAIROBI COUNTY
OMOLO FRANCIS OMONDI
Submitted in partial fulfillment of the requirements for the Degree of Masters of
Science in Mobile Telecommunications and Innovation at Strathmore University
Faculty of Information
Strathmore University
Nairobi, Kenya
February, 2015
Declaration
I declare that this dissertation is the original work of the author and all the material in
the dissertation is that is not the authors own work has been identified. I certify that this

No Service Currently Active



APPENDIX C: Screenshots

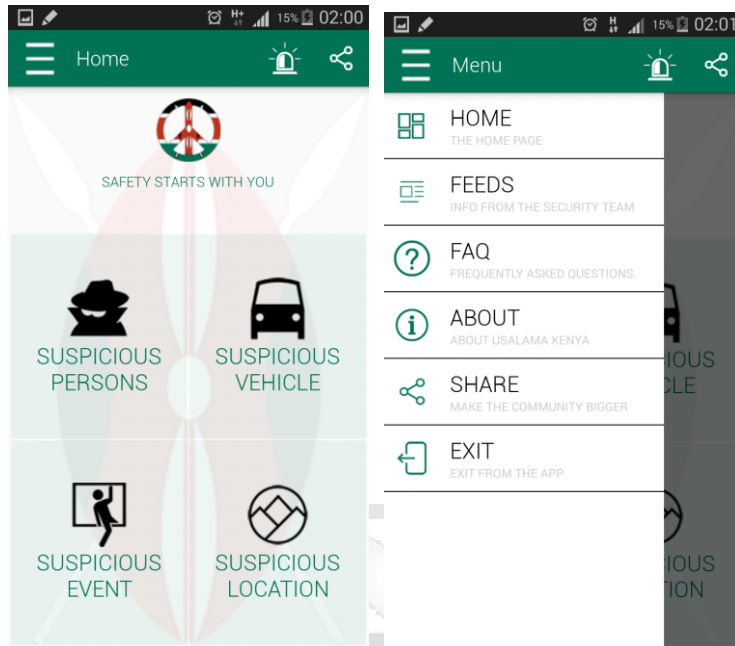


Figure B-1: The Dashboard and side bar navigation

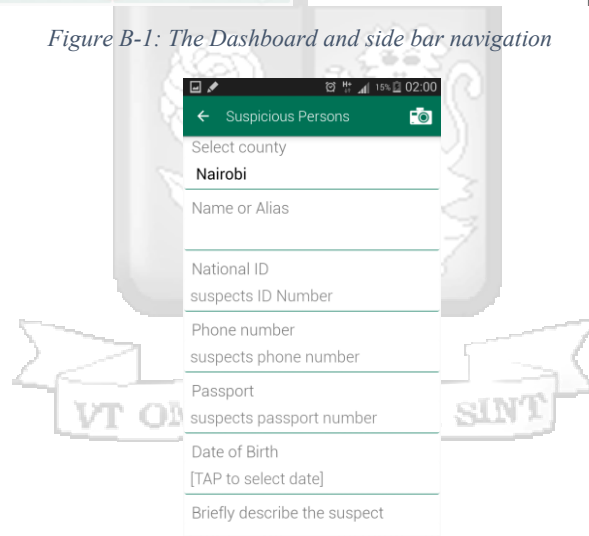


Figure B-2: The Suspicious Persons Reporting Page

Suspicious Vehicle

Select county
Nairobi

Vehicle registration plate

Make of vehicle

Last seen location

Vehicle description

Any additional information

SUBMIT

Figure B-3: Suspicious Vehicle Page

Suspicious Location

Select county
Nairobi

Describe the location of suspicion

Describe the suspicion

Any additional information

SUBMIT

VT OMNES QUOS SINT

Figure B-4 Suspicious Location Page

Suspicious Occurrence

Select county
Nairobi

Describe the place of occurrence

Describe the occurrence

Any additional information

SUBMIT

Figure B-5: Suspicious Occurrence Page

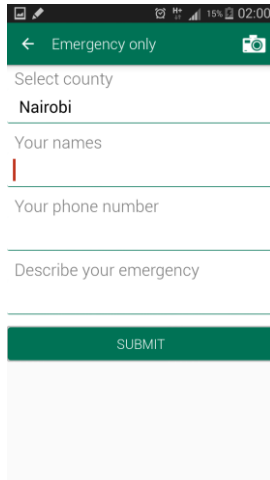


Figure B-6: Emergencies only form

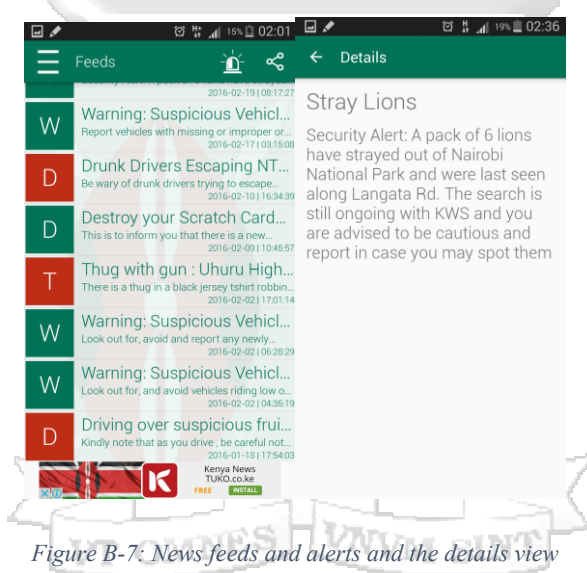


Figure B-7: News feeds and alerts and the details view

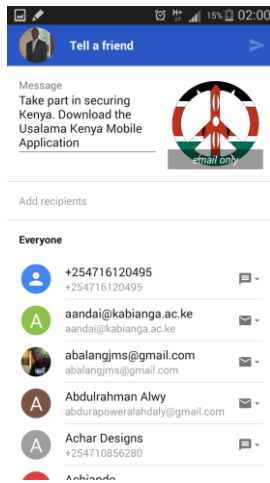


Figure B-8 Tell a friend activity

Places all places

all places PDF CSV Excel Print Copy

Show 5 entries Search:

| id | County | Location | Description | Status | Actions |
|----|---------|--------------------|--|--------|--|
| 1 | Nairobi | Karen Mvuli Estate | there is a house with very many people | new | delete details |
| 2 | Nairobi | Karen Kenya | murder wife | new | delete details |
| 3 | Nairobi | Karen Kenya | murder husband | new | delete details |
| 4 | Nairobi | Karen Kenya | murder brother | new | delete details |
| 5 | Nairobi | Karen Kenya | murder brother | new | delete details |

Showing 1 to 5 of 1,061 entries

Figure B-9: The suspicious places log

REPORTS ALERTS HELP ABOUT

Show 5 entries Search:

| # | Message level | Title | Issuer | Actions |
|----|---------------|--|---------|---|
| 1 | information | Welcome | francis | modify details delete |
| 8 | information | New Features | francis | modify details delete |
| 9 | warning | Fake Electricians and Plumbers | francis | modify details delete |
| 10 | warning | Suspicious Persons, Luggage and Vehicles | francis | modify details delete |
| 11 | warning | Crowded Places | francis | modify details delete |
| 12 | information | Unattended Luggage | francis | modify details delete |
| 13 | warning | Warning: Suspicious Persons | francis | modify details delete |
| 14 | information | Warning: Suspicious Persons | francis | modify details delete |
| 15 | information | Warning: Suspicious Persons | francis | modify details delete |
| 16 | warning | New Features | francis | modify details delete |

Showing 1 to 10 of 29 entries

Figure B-10: Alerts already submitted

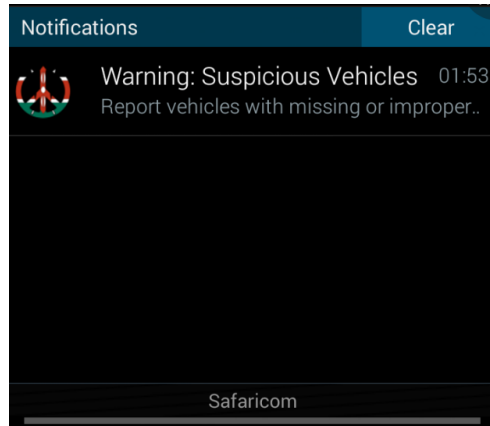


Figure B-13: The push notification

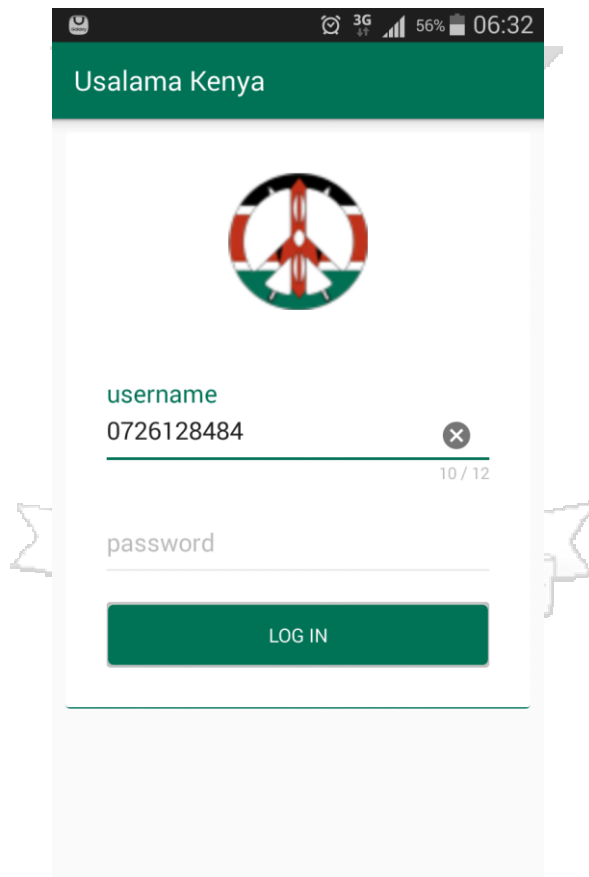


Figure B-13: The user sign in form

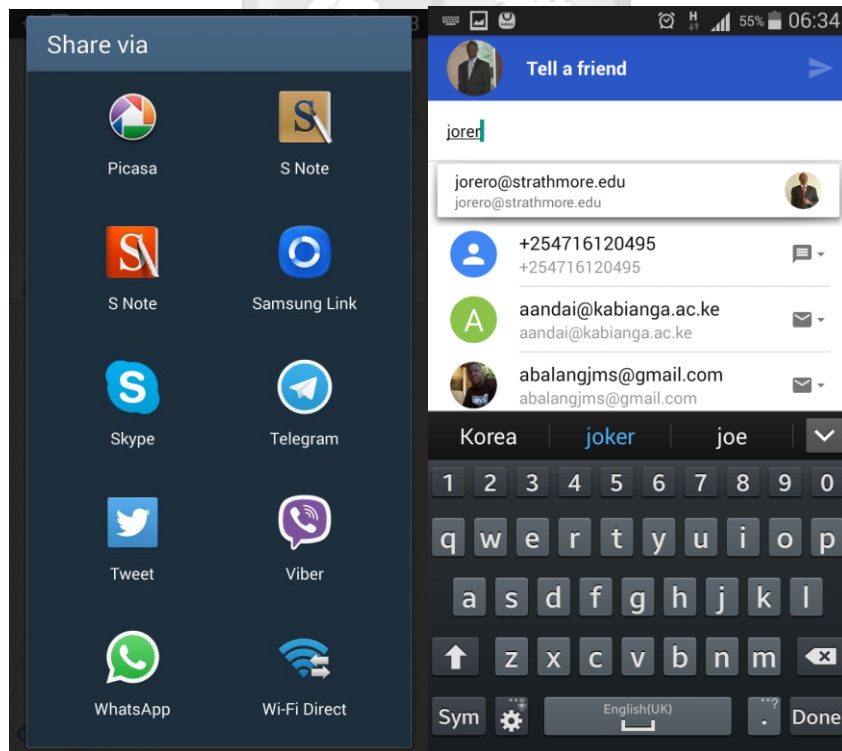
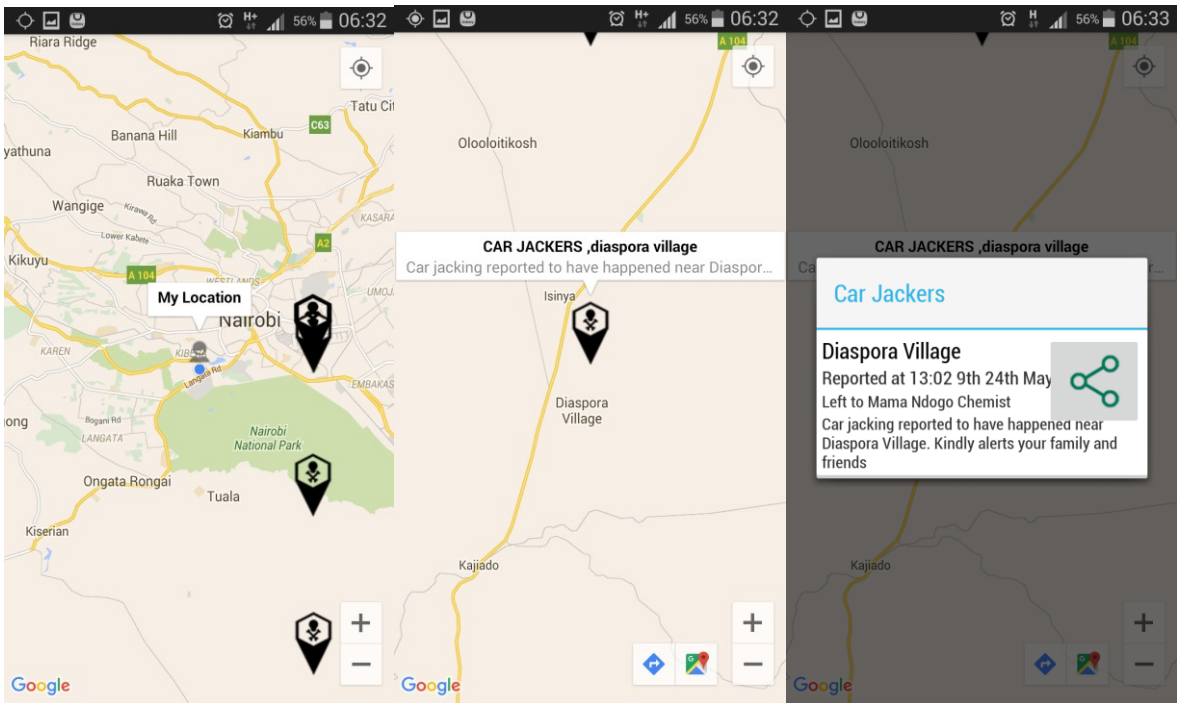




Figure B-14: The Map Threat Alert

APPENDIX D: App Invite Email Sample

Take part in securing Kenya. Download the Usalama Kenya Mobile Application Inbox x

 **francis.o.omondi@gmail.com**
to vaziani (v)


Feb 2 ⏪ ⏩



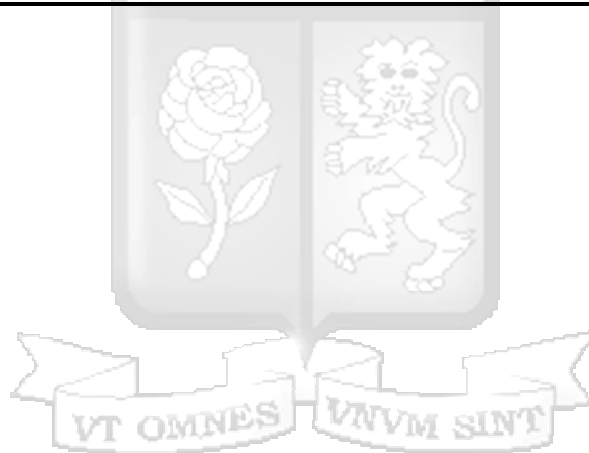
Usalama Kenya
mobilepresence

App Ratings:

★★★★★ (2)
Play Store [Install!](#)



Usalama Kenya is a intelligence gathering mobile application that enables the citizens of the Republic of Kenya to report and give leads to any suspicious persons,motor vehicle and activities



APPENDIX E: Android Play Store Application Search

