AUTOMATION AND SECURE BIRTH CERTIFICATE REGISTRATION AND MANAGEMENT PROCESS BASED ON BIOMETRICS AND QR BAR CODES

By

LUBASI KAKWETE MUSAMBO

A dissertation submitted to the University of Zambia in partial fulfilment of the requirements of the Degree of Master of Engineering in Information and Communication Technology Security.

THE UNIVERSITY OF ZAMBIA

LUSAKA

2019

DECLARATION

I, Lubasi Kakwete Musambo hereby truthfully declare that I am the sole author of this report and all its contents are my original work that has before not been presented at any learning institution for an award. I further acknowledge that similar work has been done but not exactly the same as this. All the work of other persons used to successfully complete this project, has been duly acknowledged and properly referenced.

SIGNED:……

LUBASI KAKWETE MUSAMBO

Author

This project is submitted for examination and registration with my competent approval as the Supervisor for LUBASI KAKWETE MUSAMBO.

SIGNED:……

Dr. JACKSON PHIRI.

Supervisor.

APPROVAL

This dissertation of LUBASI KAKAWETE MUSAMBO has been approved as fulfilling the requirements or partial fulfilment of the requirements for the award of the Degree of Master of Engineering in Information and Communication Technology Security by the University of Zambia.

Examiner 1:

Name:

Signature:

Date:

Examiner 2:

Name:

Signature:

Date:

Examiner 3:

Name:

Signature:

Date:

Chairperson:

Board of Examiners
Supervisor:

Signature:

Date:

ABSTRACT

This study proposes automation of the Zambian civil registration process of Birth and National Identity Card by incorporating biometrics, geospatial and encryption. In Zambia, The Ministry of Home Affairs processes civil registration in two ways: urban and rural. Both registrations initiate with the collection of a birth event on a non-standard birth source record. The birth source records are authenticated when applying for a birth certificate or a national identity card by The Government of the Republic of Zambia Affidavit Form N sworn by a commissioner of oaths. By implication, a commissioner of oaths can authenticate anyone based on Affidavit form N. This authentication process presents information security risks such as identity theft. Zambia, like many developing countries still utilize manual systems to process birth certificate and national identity card information. The first objective of the study was to determine the challenges in the current business processes leading to successful registration of birth certificates and National Identity Cards using ISO 27001 and ISO 24745 as information security and biometric security standards respectively. Based on the results from the first objective, the second objective proposed the development of a business model for birth certificates and national identity card registration using secure two-factor authentication, QR barcode, encryption and geospatial technologies. The third and last objective of the study was to develop a prototype based on the model in the second objective. A baseline study was successfully carried out and a model for the automation, secure registration and storage of civil data developed. The security features in the proposed model are based on biometrics, encryption and QR Barcode Technologies. Validation tests on the developed prototype were carried out and the results were successfully published in the IJACSA Journal vol.9 No.5 of 2018. Therefore, all three objectives of this study have been met. This model has been designed to improve civil registration in the Republic of Zambia but can be adopted to other countries.

Keywords: Vital-event, Vital-statistics, Authentication, Biometrics, Two-factor authentication.

DEDICATION

This piece of work is dedicated to God above all else.

To my wife Mwamba K. Musambo, ever scintillating and above all supportive. To my two children, Tumelo J. Musambo and Liseli J. Musambo, your encouragement is ever amazing.

ACKNOWLEDGEMENTS

Foremost, I wish to acknowledge the excellent academic guidance received from my supervisor Dr. Jackson Phiri.

To Dr. E. Mwanaumo and Dr. E. Banda, I thank you most sincerely for the insightful lessons in research and project writing; I am forever indebted to you for this knowledge.

To Dr. E. Musonda, I thank you most sincerely for the skill of preparation of a presentation that you shared with me, this, I will forever cherish. To Dr. C.S Lubobya, the encouragement that all things are possible was a thrust I very much needed.

To the entire School of Engineering staff, I am thankful to you for the learning environment you continue to create that allowed me to learn in a comfortable space.

To my classmates, thank-you all for the fellowship you created and valuable help you advanced to help me achieve this task, in particular Michael Ngala, I single you out as a true brother. Indeed, we are friends with a purpose.

To my friends from other circles, that gave me time and space to study, I most sincerely thank you, and in particular I would like to thank Mr Clarence Mulundano for your support on preparing me for the *'big talk'*, Mr Tinashe Emmanuel Lungu for that help on understanding python and Ms Chisha Mutale for that help on data collection.

I also appreciate the critique and advice from the staff at University of Zambia, School of Engineering and The Department of Computer Science under the School of Natural Sciences.

Finally to my valuable family for according me the time and opportunity to complete this task, you gave up your space and time for me and that I cannot compensate for. In particular I would like to thank Manengu Musambo for your informed direction. Thank you so much. You are priceless and irreplaceable.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

2FA	Two-Factor Authentication
API	Applications Programming Interface
ASCII	American Standard Code for Information Interchange
BIPA	Biometric Information Privacy Act
BWP	Botswana Pula
CCPC	Consumer Protection Commission
CEO	Chief-Executive Officer
CISSP	Certified Information Systems Security Professional
COBIT	Control Objectives for Information Related Technologies
CRVS	Civil registration and Vital Statistics
CSO	Civil Society Organisation
DCNR	Department of Civil and National Registration
DNRPC	Department of National Registration, Passport and Citizenship
FAR	False Acceptance Error
FRR	False Rejection Rate
GRZ	Government of the Republic of Zambia
GSMA	Global System for Mobile Communications
HTML	Hyper-Text Mark-up Language
ICAO	International Civil Aviation Organization
INRIS	Integrated National Registration Information System
ISMS	Information Security Management System
IEC	International Electrotechnical Commission
ISO	International Standards Organisation
JSI	John Snow Initiative
MFA	Multi-Factor Authentication
MLHA	Ministry of Labour and Home Affairs
MoHA	Ministry of Home Affairs
MoH	Ministry of Health
MySQL	My Structured Query Language
NRC	National Registration Card
OOSA	Object-Oriented Systems Analysis
OOSD	Object-Oriented Systems Development

OOSDLC	Object-Oriented System Development Life Cycle
OOSDM	Object-Oriented Systems Development Methodology
OpenCV	Open (Source) Computer Vision
PHP	Personal Home Page
PII	Personally Identifiable Information
QR	Quick Response
RX	Receiver
UI	User Interface
UK	United Kingdom
UML	Universal Modelling Language
USA	United States of America
USB	Universal Serial Bus
SADC	Southern African Development Community
TX	Transmitter
UN	United Nations
UNZA	University of Zambia
WHO	World Health Organization
XML	Extensible Markup Language
ZABS	Zambia Bureau of Standards
ZDA	Zambia Development Agency
ZICTA	Zambia Information and Communications Technology Authority

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

The following chapter is an introduction of the research study. The subtopics contained in this chapter are: Background to the study, statement of the problem, aim of the study, objectives, research questions, significance of the study, scope of research, and ethical considerations prior to the summary of the entire chapter.

1.1 Background to the Study

The Government of the Republic of Zambia (GRZ) through the Ministry of Home Affairs records the births of all new born babies by applying the births and Deaths Registration Act [1] [2] [3] [4]. A birth occurring in a hospital (or in an urban setting) is recorded on what is called a hospital certificate (sometimes referred to as a birth record) confirming the birth details [5]. There is no evidence to suggest that a standardized birth record format or hospital certificate exist. The parents to the child take it upon themselves to formalize the child's birth by acquiring a birth certificate through a process of notification and registration by submitting the earlier created birth record to a designated Ministry of Home Affairs (MoHA) Office [5] [1]. A birth certificate is then processed and made available to the informant or parent to a child to keep securely. The process of civil registration uses multiple documents. Among the documents include birth record, affidavit of birth (Form N) and application forms. The vital statistics registration process begins at multiple points such as Hospitals, Boma Centres, Schools, village authority centres and others declared by government. Citizens are expected to locate such centres to have their details created into a GRZ data item in order for them to qualify for a birth certificate.

The parents to a child born in a village or rural Zambia must register the child's birth in a village register apart from obtaining an under-five children's clinic card for the child at any nearest health centre within one month of birth [6]. The details recorded on this under-five card and the village registration provide support to a parent when a acquiring a birth certificate. Further, the parents to the child must also obtain an affidavit form from the nearest MoHA office and ensure a commissioner of oath provides a sworn an authentication of the

birth details [4]. Depending on parents' resources and capability plus considering the need to travel to and from the registration office, the whole process of acquiring a birth certificate can be mathematically ambitious to determine in terms of time and finance as soft factors and others may impede the process from a parents' perspective [7].

At an age of 16 a Zambian is entitled to a NRC (National Registration Card). This can be secured from The Ministry of Home Affairs, Department of National Registration and Citizen Registration [2] [1] [8] [4] .There is need here of the individual to locate a designated GRZ office executing the registration process and acquire the NRC. A birth certificate is needed in addition to a sworn affidavit. Hidden costs will follow this transaction such as those for a commissioner of oaths during authentication of the affidavit.

This study, therefore, proposed to develop a secure biometric software model based on ISO 27001, ISO 24745 for birth records and NRC that automates the current manual processes of civil registration. To ensure vital data relating to the vital statistics are secured, encryption, QR Barcode and geospatial technologies would be implemented.

1.2 Statement of the Problem

Two-factor authentication is the use of more than one piece of datum or technological tool to identify and bind an entity to a transaction [9].The consequence that during a Zambian National Election, multiple individuals exist with shared NRC Number details or an NRC that cannot be traced to a birth [10] shows a problem of authentication, integrity and a possible failure in non-repudiation. Further, the fact that individuals share an NRC number [11] indicates issues of a failure of secure storage management and a lack of a centralized database plus supporting applications to manage the information distribution processes. There is also a possibility of data theft and identity theft with far reaching consequences.

A failure to track an NRC to an actual vital event or birth of an individual, the failure to produce sequential numbering that rids the system of duplicate NRC numbers, the failure to securely store the NRC details of an individual are issues that require address. These problems have an extended linkage problem of association rule mining [12]; once an erroneous data item about an individual is captured by the current system it becomes the basis for further decisions, these decisions such as acquiring a Zambian passport or opening a bank account and others are all made with an error emanating from a wrong vital event captured at data

creation point. The fact that vital event data is kept at source presents a possible information security risk of record alteration or destruction [13]. There was, therefore, need to overcome these challenges.

1.3 Aim of the Study

The aim of this study was automation and secure birth certificate registration and management process based on biometrics and QR Bar codes.

1.4 Objectives

The study objectives of this research were to:

i. Determine challenges and business processes in the production of birth certificates and NRC based on ISO 27000, ISO 24745;
ii. Develop a business model based on findings in (i) for birth certificates and NRC storage and
iii. Develop a secure 2FA Biometric model based on findings in (ii).

1.5 Research Questions

For the purpose of this study the following research questions were formulated;

i. What is the level of ICT utilisation by GRZ in vital Data management based on ISO 27001, ISO 24745?
ii. What are the limiting factors that GRZ encounters in setting up a secure ICT Biometric System?
iii. What ICT secure model can be developed to capture and process vital statistics?

1.6 Significance of the Study

This study proposes to give an improved method to the collection of vital statistics in a secured way by employing biometrics, encryption, geospatial, QR barcodes and two-factor authentication.

1.7 Scope of Research

The research was focused on understanding how 2FA can be applied to biometric civil data. This study was conducted within the city of Lusaka as this is the capital city Zambia which also happens to be the headquarters of most of the organisations in Zambia and, therefore, represents the general view of the branched organisations outside this city.

1.9 Ethical Considerations

This research utilises personal data that can be used to identify an individual and bind an individual to an event or transaction. Due to the nature of the research data used in this research topic and the sensitivity of the information that was required for this research, guidance from the University of Zambia was sought. Consent from research participants and organisations was equally sought in the use of personally identifying information. Consent to collect human statistic data from all individuals that were selected to participate in this research project was obtained. All human identifiable information collected was treated with care and confidentiality of the utmost. All participants were made to understand that the data collected from them was to be used for research purposes only. The researchers endeavoured to function with a high level of integrity and professionalism due to the sensitivity of the information which was acquired.

1.10 Summary

The contents of this chapter focused on the dissertation introduction. This chapter has highlighted some of the critical reasons behind the need to develop a workable model that may be used to capture and authenticate biometric data in the vital statistics arena. The chapter has pre-empted the region of literature to be further studied in the following chapter.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter contains different literature reviewed from various academic, Government and industrial sources. The various sources include journals, conference papers, reports, text books, government documents and selected items from the internet. The chapter is presented to cover the thematic areas of the research study. The areas of discussion range from a general discussion on civil registration management covered comparatively by looking at countries under study and which civil biometric tool has been implemented. The chapter discusses challenges in civil data management per country under study. The chapter also explores standards in line with biometrics and ISMSs. Aspects of QR barcodes are also discussed and married to civil data management.

2.2 A Perspective on Civil Registration Processes

Various literature taken from a perspective on civil registration processes has been examined.

2.2.1 The Elements of a Civil Registration Process

Figure 2.1 shows the generally accepted civil registration process as defined by Taylor [14].

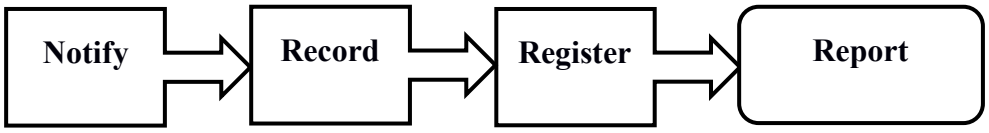


Figure 2.1. Vital Statistics Approach. Adapted from [14]

As shown in Figure 2.1, an ideal Civil Registration system must have capabilities for:

i. Notification: where the Government units responsible for the collection of vital data are made aware of a vital event such as a birth;

ii. Record: where the Government units that are responsible for the collection and retention of vital records such as a birth certificates and NRCs are given data relating

to those vital events which they then retain;

iii. Register: where the Government units responsible for the collection and management of vital data records generates vital event documents such as a Birth Certificate and NRC that they make available to the informant (the individual who performs the notification of the vital event to the Government).

iv. Report: the civil registration unit accounts for its' activities to government and citizens.

Vital events refer to situations or circumstance concerning the life and death of individuals. These events also refer to the family and civil status of those individuals. These events occasioning around an individual form basis for their recording. Governments and countries have interest in the events of individuals or citizens as this information is used for economic planning. These units of information provide important information on the population in a country. In accordance with Chapter 51/5 of **The Births And Deaths Registration Act of the laws of Zambia** established under **The Constitution of Zambia (Amendment), 2016-Act No. 2** as amended in Principle, registration of every vital event occurring within the boundaries of the country of Zambia MUST be made legally compulsory for every group of the population and parallel provision for enforcement should be established [15]. These vital data elements form what is referred to as civil data. In Zambia, a Registrar-General of Births and Deaths for Zambia, and a Registrar of Births and Deaths for each district are appointed to identify, classify and collect vital statistics [5].

It can then be deduced that vital statistics (civil data) will encompass: live births, deaths and fatal deaths, marriages, registered partnerships, separations, divorces, legal dissolutions of registered partnerships and annulment of marriage, as well as adoptions, legitimation and recognition.

According to the Classification of vital statistics done by adopting the National Statistics Institute, two paradigms can be adopted to classify vital statistics, these being Marriage and Death [16]. Clause 8 of the birth and death registration act of the laws of Zambia, however, classifies vital events into birth (still-born or not) and death [15] [5].

'A vital statistics system is defined as the total process of (a) collecting information by civil

registration or enumeration on the frequency of occurrence of specified and defined vital events, as well as relevant characteristics of the events themselves and of the person or persons concerned, and (b) compiling, processing, analysing, evaluating, presenting and disseminating these data in statistical form. The vital events of interest are: live births, adoptions, legitimations, recognitions; deaths and foetal deaths; and marriages, divorces, separations and annulments of marriage' [8].

Countries around the world register their citizens so as to make it easier to identify and separate individuals. Several practices are entered into to register or record details about an individual [17]. Normally the registration or recording of an individual may be done soon after birth or in some cases may be done sometime after a person has been born [18] [19].

Registration or recording of individuals is important as it provides a means for a country to know its citizens and helps the country in terms of its economic, social, health, education planning and others [8]. In certain circumstances an individual may not be allowed access to schools, University or even sit for exams without a birth certificate. This implies that vital statistics must be captured and must be accurate [20].

Countries such as America register their individuals by following rules of the state where that individual is born [21]. In the UK (United Kingdom) registration of an individual is done at the hospital of birth or an alternative registration recognised by the government [22]. In Africa, though vital data management is unsatisfactory, several approaches apply for instance, in Libya registration of an individual is done by following law Number (24) for 2010/1378 on Libyan Nationality. By following this law, and with the development of IT infrastructure, the government has ensured that each municipality has its civil registration office where birth, marriage, divorce and death must be registered. The civil registry records are known to consist of many unauthenticated family books and records. It can be seen here that an issue of entity binding is a problem (failure to authenticate). According to the "The Libya Herald", the civil records are in a bad state and as such the current civil registration system must not be fully accepted [23]. Out of 13 countries researched by the SADC (Southern African Development Community) on vital records management, a general conclusion is made of how the process is somewhat not well coordinated and as such further work must be done in this area [8]

All the above registrations have one thing in common; the need to accurately capture an aspect of an individual early enough in the life of that individual so as to create a history for that

person which can be used to identify and bind that individual to a his / her birth.

In the Republic of Zambia, the Ministry of Home Affairs (MoHA) is charged with the responsibility of registration of Citizens in Zambia and registers the births by using the births and deaths registration act [4].

2.2.2 Civil Registration Systems and documents

Starting with the UN, a comparative study of the civil systems that are used by different African countries together with their vital documents is presented. This author presents an overview of the challenges and types of vital documents in the civil registration systems in the studied African countries by understanding them from the UN's perspective. A brief study of the European Union's perspective on its' civil system made is so as to demonstrate comparison. The study on African countries is focused on their challenges and the solutions they have developed in terms of the management of vital data. The countries studied include Botswana; Tanzania, Ghana and lastly Zambia.

2.2.2.1 The UN Perspective

The United Nations (UN) through its' Statistical Paper Series M No. 19/Rev3 which sets standards for civil registration highlights some of the important aspects that must be born into a civil registration system. Figure 2.2 illustrates the elements of a vital statistics system according to the United Nations. Among the issues highlighted include [24]:

i. Integration processes must be built into the civil registration and vital statistics systems;
ii. Uniform legislation and regulation nationwide in centralised or decentralised environments; civil registration systems must be regulated upon in a uniform manner. Basic policy and procedure must be uniform in every part of a country;
iii. Regardless of whether a centralized or decentralized registration system model is in use within a country, it is essential that there be in place uniform registration laws and regulations which establish the basic policies and procedures so as to allow for clear international and national interpretation;

iv. Civil registration systems and the users of the civil registration systems must be able to coordinate using uniform approaches that must be followed at every level. This will result into quality;

v. A well-coordinated public awareness program must be in place to avoid public misconceptions and loss of public trust and

vi. A well-educated local civil registrar who receives training often to ensure consistent service delivery to citizens.

The technical report further present solutions to the many challenges a country such as Zambia faces in the civil registration process but does NOT offer a particular standard that may be adopted by countries. It encourages practices within laws and civil registration policy set out.

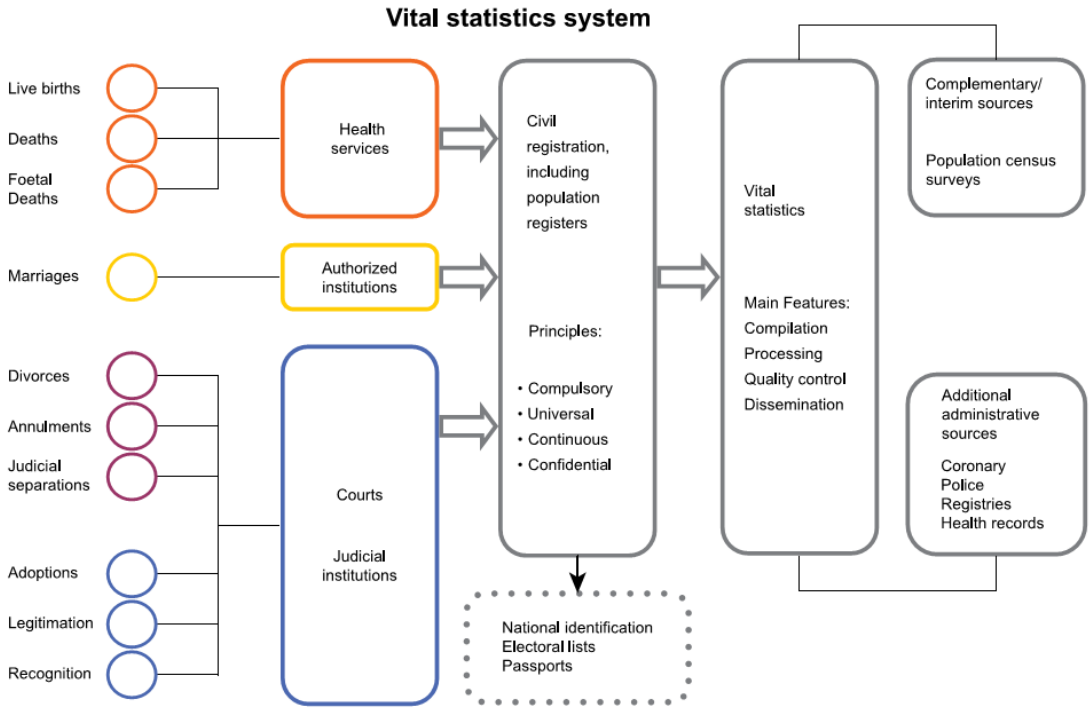


Figure 2.2. Vital Statistics System [24]

2.2.2.2 The European Union Perspective

Figure 2.3 shows a typical identity card valid for the EU (European Union) region. The card is developed with an embedded microchip which holds biometrics in form of fingerprints of the holder and other personal details such as name, sex and place of birth among others. The card is colour coded to reflect the region (pink for EU while blue for UK). The card is also developed with digitized images of the holder and a dynaprint feature (colour change feature depending on angle of view and light opacity.

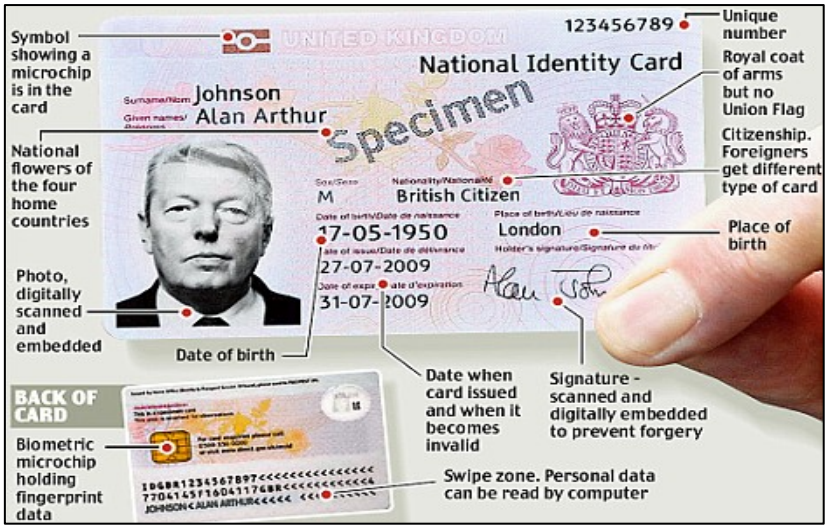


Figure 2.3. EU Sample Identity Card. Source: [25]

The cards are accessible to all deserving individuals within the EU depending on factors of longevity of stay, ability to speak a national language, marriage, ancestry, investment or others that the country awarding the citizenship may deem necessary [25] [26].

2.2.2.3 The Botswana Perspective

In Botswana, civil registration involving birth is equally compulsory just like in Zambia [19]. Civil registration involving births are performed by the Department of Civil and National Registration (DCNR) at the Ministry of Labour and Home Affairs (MLHA) [27]. Two processes are followed in order to perform a birth civil registration depending on whether the registration is on time (within 60 days of birth) or is a late registration (60 days or more after birth) [27]. In an *'On time registration',* Registration can be done either at the health facility where the birth occurred or at the nearest DCNR office. For a registration at a health facility, health personnel collect all birth details onto a birth notification form and transmit it to a DCNR office for further action. This is performed within an hour of birth or within a week of birth at remote sites (Districts). At the DCNR office, the form details are entered into the Births and Deaths Registration System, where registration is quality-checked and authorized. This completes the registration and a birth certificate is made available to the informant [19] [27]. For all late birth registrations, fees are applied as follows: A late registration fee of BWP 5 is charged for every month of not registering up to a maximum of BWP 100. For a duplicate certificate, BWP20 is charged, while for alterations the fee is BWP 10 [27]. Technological

divide has been determined to be a contraceptive to rural birth registration. This challenge forces a belief that rural areas have a low birth rate [19]. The government of Botswana has however, provided networked facilities to enhance on-line registration. Quarterly outreach visits have been embarked on to improve the registration of births in rural areas. To eliminate identity fraud factors, the government in Botswana has enhanced the birth certificate paper features for the purposes of providing information security and quality on the birth registration papers [19] [27].

Challenges in Botswana civil registration process as identified by Poloko [19] and MLHA [27] [28] are:

i. Incomplete registrations;
ii. Civil records are at variance with reality and this results in poor association-rule mining;
iii. Incomplete coverage of marriages (traditional marriages); this may result into a neglect of capturing birth events born to those unrecorded marriages as they are ignored;
iv. Parents or informants do not see the benefit of registering a birth or do not have the parental enthusiasm for birth registration;
v. Shortage of equipment and human resource to register births all across the country and
vi. The geographical terrain is difficult to negotiate in certain remote areas.

Figure 2.4 shows a sample copy of the birth registration notification form used in Botswana.

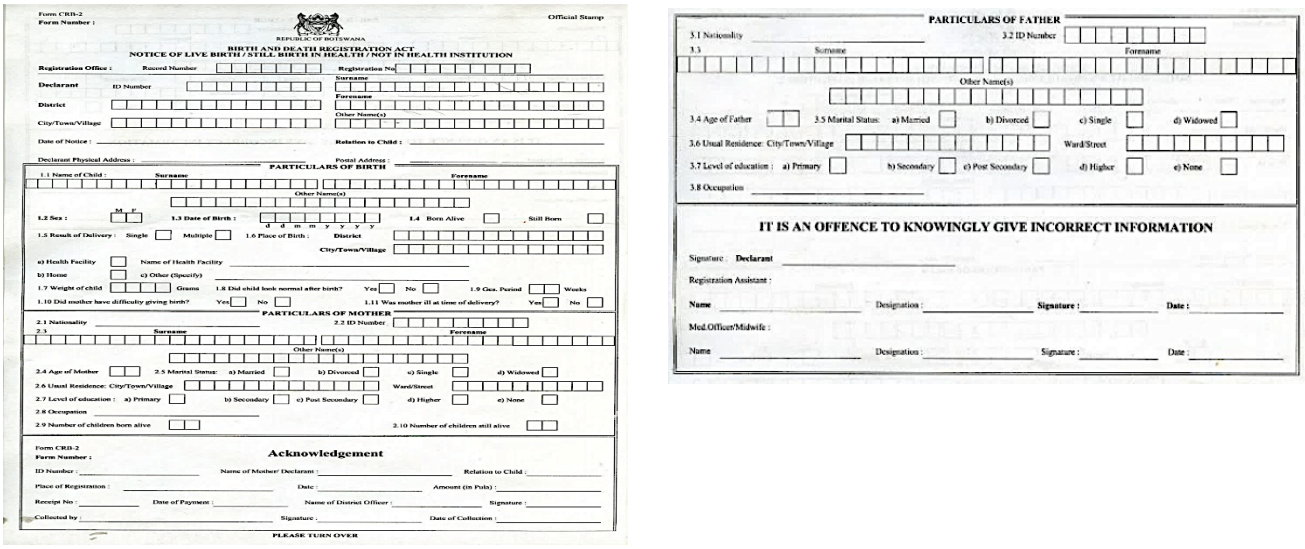


Figure 2.4. Birth Notification form. Source: [169]

Figure 2.5 shows the Tswana (Tswana is name for indigenous people of Botswana) OMANG (national identity card) civil registration process. Figure 2.6 shows the OMANG card.

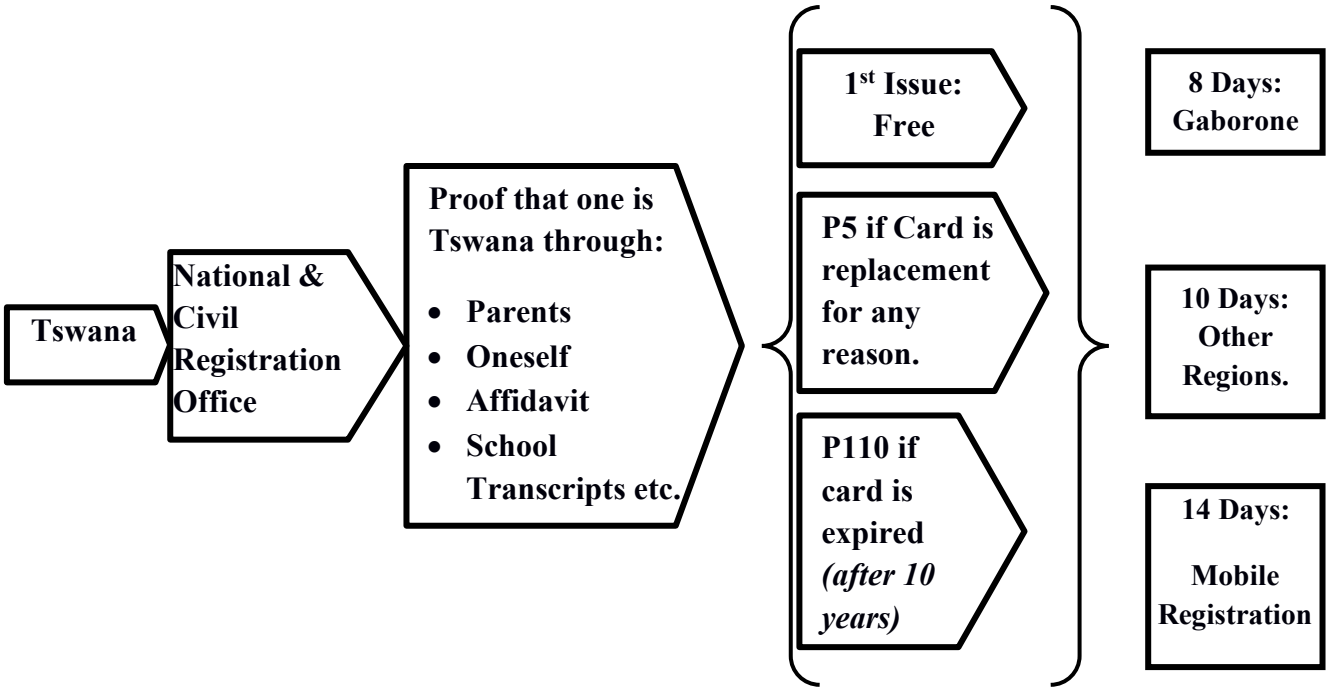


Figure 2.5. OMANG civil registration process [28]

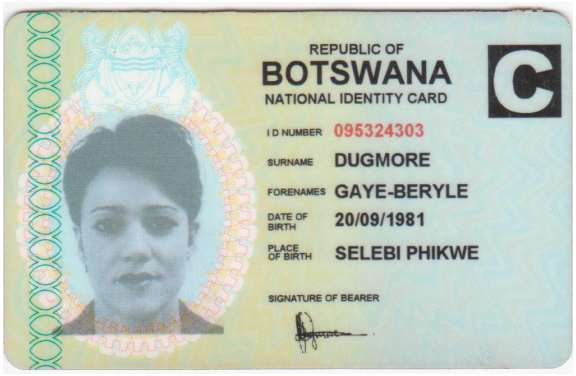


Figure 2.6. Sample OMANG card. Source: [170]

2.2.2.4 The Tanzanian Perspective

In Tanzania, birth registration is mandatory and enforced by *'The birth registration process established through the Births and Deaths Registration Act (2002)'*. Charges apply for registrations in either case of early or late registration. Information amendment fees equally apply [29].

Challenges of birth registration as stated by GSMA [29] and Mtulya [30] are as follows:

i. A large population of individuals are born outside a hospital facility (at home);
ii. There is only one registration office per district out of 169 districts;
iii. Distances to the registration centers impede the registration process;
iv. Technological divide provides a limitation in rural areas;
v. The process is deemed time-consuming, expensive and inconvenient and
vi. Parents generally lack awareness about how to complete the registration process and the rewards that come with the registration.

To overcome these challenges the Government of Tanzania has embarked on the development of a strategy to capture all citizens through the use of mobile phone technology [31]. This initiative referred to as The Under-five Birth Registration Initiative (U5BRI) aims to address challenges around birth registration across the country of Tanzania by making it easier for parents to get birth certificates for their children because the health facilities and ward executive offices have been turned into registration points.

The Tanzanian National Identity card is shown in Figure 2.7. The card was successfully launched in 2013 though planning and other initiation activities started as early as 1968 [32]. The identity card uses finger print and retina biometrics. This method of citizen capture is meant to prevent identity theft [32].

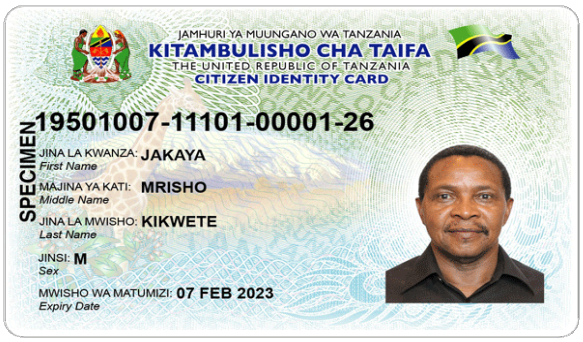


Figure 2.7. Sample Tanzanian Citizen Identity Card. Source: [168]

2.2.2.5 The Ghanaian Perspective

In Ghana, the civil registration of births started in 1912 with incremental improvements along the way. The Births and Deaths Registry Act 301 of 1965 and the Registration of Births and Deaths Regulation LI 653 of 1970 of the laws of Ghana, manages and maintains all data

and information relating to births and deaths. Certificates relating to births and deaths are issued by following this law. This law also develops frameworks in the civil registration sector that manage the registrations and ensures integrity of information as far as births and deaths are concerned [18] [33].

The civil registration centers are divided into 10 registration regions and sub-divided into 110 registration districts. A registration office manned by District Registration Officers supervises the registration system through the registries and reporting centres in each district. Registration Officers on a monthly basis submit registration forms organized serially to the Regional Registration Office for processing and further transmission to the Central Registry Office for national data collection. Copies of source records for registrationn are maintained at all the 3 levels to secure the information for development activities (district office, Regional office and national office) [33].

Figure 2.8 illustrates the business processes in the Ghana birth civil registration system.

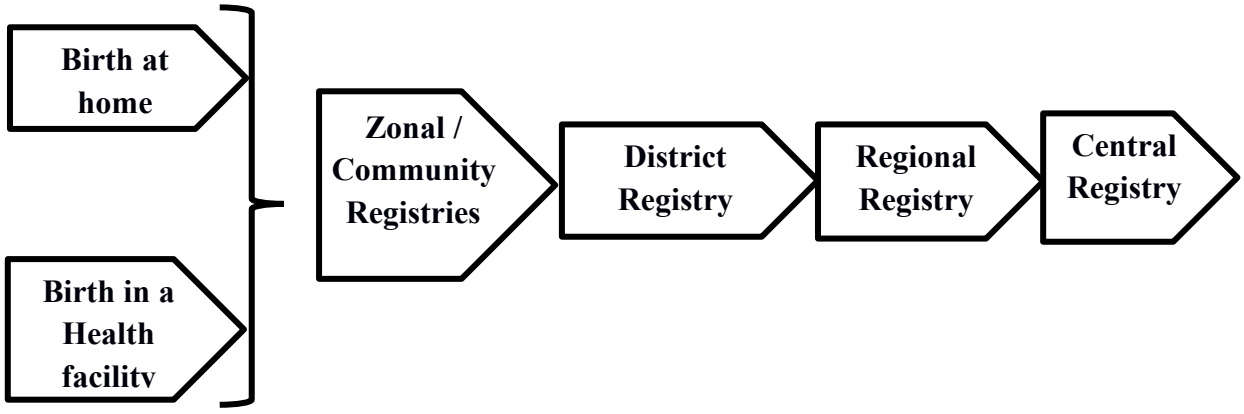


Figure 2.8. Ghana Birth Civil birth Registration. Adapted from [18]

The birth of every child must be registered in the district where the birth has occurred. A child's surname is taken to be that of the father. Child registration is mandatory and must be done by a parent to the child or guardian or any other individual who has charge of the child at birth. The individual registering the birth is referred to as an informant. A birth certificate is issued after the registration of the birth and no charges are imposed at this stage if the registration is within 1 year of occurrence of birth [18]. Registration outside this period attracts a prescribed fee but is allowed up to 59 years of age [18]. Hospital based registration is not supported by law but is done by informal agreements to ease the stress of registration bureaucracy [33] [18].

Challenges in the Ghana civil birth registration system can be summarized to:

i. Legal limits imposed by the law [33] [18];

ii. Missing legal provision for electronic systems birth registration [18];

iii. Linkages in the registration centers appears amiss;

iv. Minimum requirement for proof of birth is amiss in the law;

v. The name of a parent is a requirement in the registration process. Should a registration be attempted but a parental datum is missing a challenge suffices [18];

vi. Low coverage of births registration;

vii. Inadequate funding to the registration center;

viii. Multiple registration of birth [33] and

ix. Poor education of the population in the processes of registration.

Figure 2.9 shows a sample of a national identity card used in Ghana which an individual can acquire from an age as low as Zero (0) years [34]. The card is developed around finger print biometrics and collects all ten finger prints of an individual in addition to the facial image and a dual interface chip module that supports 128Kb data storage capacity [34].

Figure 2.9. Ghana ID card Sample. Source: [37]

2.2.2.6 The Zambian Perspective

In the Republic of Zambia registration of all births is compulsory [1] [35]. Civil registration is conducted by the MoHA. Zambia has the lowest civil registration in Africa [36] [37].The

current civil registration in Zambia stands at 11.2% of the population which translates to about 1.9 million registered individuals and the other 15.2 million not being registered since the population as at end of 2017 stood at approximately 17,094,130 [36] [38] [39]. Zambia's population is divided into the female population which is greater, with 8,611,904 women, representing 50.38% of the total, compared to 8,482,226 or 49.62% men [39]. Kambole et al. [35], discusses at length the processes undertaken in the Zambian civil registration process. These processes highlighted are the activities undertaken in the creation and storage of the civil data and the levels of confidentiality expected from the registration officers. A summary of the problems as discovered by Kambole et al. [2] are as follows:

(i) Shortage of manpower;
(ii) Delays and inertias experienced in the delivery of birth notices from registration centers;
(iii) Transportation problems of vital documents from remote areas to central processing centers for birth certificate preparation [37];
(iv) Amendments to informant data takes long to amend due to the manual operations undertaken and a lack of a citizen database. This results into certificate purging resulting into high costs for GRZ;
(v) Inefficiencies, delays and uncertainties in the production of birth certificate and NRC paper;
(vi) A lack of citizen awareness of the processes of civil rregistration and
(vii) A lack of motivation system for the employees involved in the civil registration process.

In their work, Kambole et al. propose several solutions among them are human resources-based solutions. These solutions are aimed at overcoming issues of shortage of labour. Issues of citizen unawareness are presented, and a solution of regular national sensitization is presented to counter this problem [2] [37]. To ensure employee engagement into the civil registration process, this work also proposes employee motivation structured on a spectrum of human resource motivation is implemented as a way to mitigate some of the challenges inherent in the civil registration system. In the Kambole et al. submission, issues of information security are not covered, and neither is any recommendation of a framework based on internationally accepted standards or framework to manage the civil data especially the biometric data.

The government of Zambia through the MoHA is currently implementing interventions to counter the challenges of civil registration. In the National Strategic Action Plan for Reforming and Improving Civil Registration and Vital Statistics [37], MoHA lists the following intentions that it hopes to realise by the year 2020:

a. Improving the availability and accessibility of civil registration services by decentralising registration facilities to local levels in 2 ways namely [i] Integration of the health system into civil registration and [ii] Integration of the community system into civil registration;
b. Adopting appropriate technologies to speed and scale up civil registration, manage civil registration records and application of ICTs in improving Civil registration and Vital Statistics (CRVS);
c. Strengthening and simplifying synchronisation between Civil society Organisations (CSO) and DNRPC to ensure development of vital statistics from civil registration information & awareness creation and public education on the importance of civil registration and
d. Introduction of INRIS; a system that if implemented will conduct registration of citizens, verify personal information, positively identify a citizen, and provide accurate and credible reports, statistics and citizen information to authorized government agencies. INRIS shall be made up of National Registration birth and death Registration, Marriage Registration, Adoptions Registration, Village Registration, Citizenship Registration and Passport issuance.

2.3 Use of Civil Data

Civil data is enormous, and its use is equally enormous. The use of civil data may be placed into the following categories:

a. Personal use;

b. National or Government use and

c. International Use.

2.3.1 Personal Use

For personal use, civil data provides an opportunity to qualify certain data items about a

person for instance a birth record, provides documentary proof of identity and civil status touching on such matters as age, nationality (citizenship), and parentage [1].

Evidence of proof of identity is required in many countries to acquire a passport, to own property, to be employed in the civil service and participate in politics. Also, proof of age is demanded to enter schools and to seek regular employment in some countries. Similarly, the death record is required in the settlement of claims to inheritance and to insurance on deceased persons [23] [40].

2.3.2 National or Government Use

The use of vital data in government systems cannot be over emphasised as the spread of social and economic development gives a demonstrated use of vital records and emphasis their importance.

Legal, administrative and statistical use are key to Government use of vital data. Among the important administrative use of vital data for governments include:

i. Proof of identity for its citizens through the use of a birth record or a national identification system such as the NRC (national registration card) for Zambia [1] [18];

ii. Evidence of parentage is equally key for Government planning and or investigations in certain matters such as identifying parents to an individual in the advent of a crisis such as an accident [29];

iii. The government may want to identify or know who owns which property, this identification is made possible with accurate vital data;

iv. The planning of government services such as refuse management, electrical, sewage and water services planning [2];

v. The planning of employment is another critical element that vital data provides information to. Vital data directly feeds into the employment process as the government is interested in knowing how many of its citizens are at an appropriate employable age [23];

vi. The government may want to know how many individuals are born every year and

possibly how these births may affect government revenue and its provision of services. All this information is used to forecast government expenditure on its citizens. This implies that vital data is critical to government planning [22] [29] [2];

vii. Government schools entry level is partly determined by age as in the case of Zambia so vital data is a planning tool here [23];

viii. Issues of death are important for the Government as the Government is interested in planning for body disposal areas and determination of how to dispose of bodies. This is made possible by vital data in death. Further to this, death information is used in the settlement of claims (such as insurance, inheritance etc.) in arbitration issues handled by a Government [6] [23];

ix. The planning of and delivery of efficient implementation and evaluation of health-projects are determined by how vital records by a government are well kept. An extension here is that vital data can be used to monitor progress in public health programmes in such areas as the control of communicable diseases and maternal and child health projects [19] [29] [18];

x. In those countries that are inundated by the problems of external and internal population motilities (mass movements), governments are anxious to regulate these movements. Legal documentation of nationality, such as provided by birth records is one possible strategy for control that can be used [8] [23];

xi. Vital data may be used in a statistical form to work out mortality and fertility rates [29] [6] [40] and

xii. Historical vital data can be used to estimate the growth, structure and geographic distribution of the population. This information can be used in formulating and implementing programmes of social and economic development [2] [40].

2.3.3 International Use

Vital data generated by one country may be needed for use by other countries in a number of ways. A few of such reasons are as follows:

i. Internationally, vital data collected (births, deaths, marriages and others) in one

country may be needed by another country to allow it plan for it's the possible future exports to that country. Export may range from things such as foods, electronic equipment among others [18] [29] [22];

ii. Countries such as the UK, the USA, and Germany among others normally tend to help other countries (Donor-Aid) such as Zambia, Malawi and others financially, materially and through the transfer of skills. In order for such aid to have a bearing on the country being helped, it is important for the donor country to know or have some understanding about the vital statistics position of the country to be helped. This allows for planning on quantities and others. All this is made possible by the availability of vital data to the donor [18] [20] [8].

iii. The advent of discontent presented by political strife is prevalent in certain countries. In view of such, citizens of one country may flock to other countries seeking refuge. In order for the country welcoming these refugees to take account and possibly better plan for such immigrants, a brief understanding of the vital statistics position of the country refugees are fleeing from is key [41] [23] [42].

2.4 An Approach to Civil Data Security

Various methods and technologies may be used to store or retain civil data. Civil data must be kept with a bias towards Information Security.

The institutions that must store civil data must approach the issue of information security from a very informed position. In order to secure an organisation, an evaluation of the impending obstacles to the security of that organisation must be made. In his book, *"Computer and Information Security Handbook",* John Vacca suggests that it is cardinal to first evaluate the obstacles to securing an organisation [43]. In his submissions, John Vacca alleges that obstacles to the security of an organisation may be viewed from the following 8 points:

i. Security is an inconvenience;

ii. Computers are complex;

iii. Computers are created without a thought to security;

iv. Current trend is to share not protect;

v. Data accessible from anywhere;

vi. Security isn't about hardware and software;

vii. Bad guys are sophisticated and

viii. Security is a drain on resorces.

2.4.1 Security is an inconvenience

Among the multiple points of evaluation include the understanding that security is perceived as an inconvenience because in the implementation of a security protocol for an organisation, certain limitations are imposed on stuff and customers in certain cases such that their ability to function is hampered by the security innovations. An example of such an inconvenience would be a case where employees are required to have their property scanned by x-ray every morning when reporting for work. This step would add to the delay time that organisations experience every day before any actual work is done, this in turn adds to a significant time lost over a year in security details [44].

To ensure a security protocol implemented in an organisation balances with organisational performance, the implemented security measure should be placed on the scale where the level of security and ease of use match the acceptable level of risk for the organization [45] [46] [47].

2.4.2 Computers are complex

Another submission advanced is that an obstacle to securing information exists in the fact that a computing resource is a complex piece of technology that must be used with care. Among the various technologies that computing systems have in-built that is complex to a basic user is a computer communications port. These ports can be easily compromised by an attacker to steal private and business data on a computer network [43] [48]. Such complexity must NOT be forgotten or ignored but must be recognised as an obstacle to

securing vital data. Complexity like this is often overlooked or ignored but this may be a strong obstacle to securing vital data. Other forms of complexity include technological services found in certain operating systems that run computer hardware such as the Microsoft Windows operating system. Microsoft Windows supports the use of registers and other hidden services that may be compromised by an attacker to take advantage of a victim's computer and either steal information or harm that computer [49] [50]. Complexity is the obstacle.

2.4.3 Computers are created without a thought to security

The third aspect in the evaluation of security for an organisation before implementing a security protocol that wins support from multiple scholars is that computer users are unsophisticated much to the chagrin of the experienced computer user [43]. The element here is that an individual who has utilised an office application over years and has grown his or her experience in such an application may have an illusion that they are sophisticated in the use of computer systems but such individuals have no technical understanding of computer security organisations along the lines of, say, cryptography. Such knowledge missing in an individual would lead to such individuals placing their organisation in direct contact with the more sophisticated hackers by visiting unsafe web sites or installing unsafe or botnet present applications. Their long-time usage of office applications gives them the impression that they are sophisticated and yet they are NOT. Such individuals are prone to phishing attacks or social engineering attacks [51]. These average users, though, see themselves as sophisticated are equally at risk from internet attacks that come in form of botnets which have capacity to compromise computing resources in seconds to either steal private / organisational data through phishing scams [52] or simply harm the resource [53] .Harm may come in form of malware software such as the Ransomware programs that seize computing resources pending payments to the owner of the Ransomware application [50]. As an extension to this argument, the development of computers seems to be driven by what a computing device is capable of delivering to its owner and not about how it can be made secured from attacks [54] [55].

2.4.4 Current Trend Is to Share, Not Protect

The advent of applications that promote social interactions has made it possible for individuals to share content and interact in real time [56] [57]. These interactions however present individuals with an amount of risk to their information as information can be stolen by hackers or attackers who may have intentions of using such information for themselves [58] [59] [60]. Because social sites such as Facebook encourage users to share information such as text documents, images, work files (even private information) about themselves, such information is available to a third party. This exposure is risk enough to warrant theft of private information. The trend to share information though interesting at personal level must be done moderately. The loss of security of social sites is enhanced by the introduction of cloud storage systems which offer individuals an added ability to keep their information on cloud systems [61]. Cloud systems may expose an organisation or individual to further threat as their information now resides on a computer far off without physical reach of the data owner. This seclusion may also mean the owner of the server on which the data is kept may do with that information as he sees fit.

2.4.5 Data Accessible from Anywhere

Organisations and individuals are nowadays keen on securing cloud storage systems that allow them to keep or retain their information both personal and non-personal, private and public. Reasons for such are wide and varied but among the reasons include the need to have continuity in terms work, the ability to have resilience in the event of a misfortune such as a fire that destroys the current IT infrastructure base, the need to be efficient, or simply the need to appear smart (competiveness, user-friendly, automatic update to software systems or data, customer-integration etc) [62].

Though the move to cloud computing systems promises certain positives, it must also be noted that threats on information are very present on cloud managed systems and data. Naresh Vurukonda and B.Thirumala Rao present a dimension of 3 issues in their paper entitled *'A Study on Data Storage Security Issues in Cloud Computing',* that must be addressed if an organisation or individual is to use cloud storage systems for their data management [63]. Figure 2.10 illustrates the concept. Reading left to right we can draw an understanding that 3 types of cloud security challenges abound these issues are (1) data storage issues (covering issues to do with the privacy and integrity of data, ability

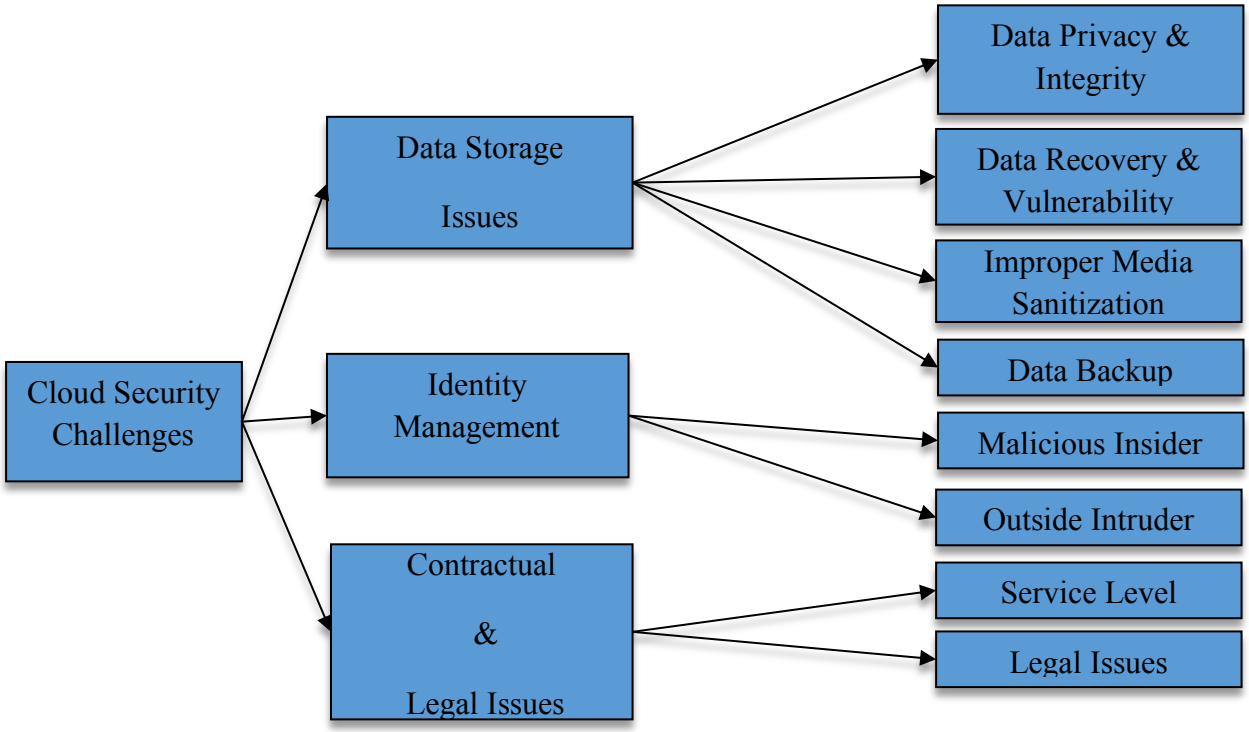


Figure 2.10. Cloud Security Challenges [63]

aspects of both the systems in place and the data itself, the issues to do with ensuring that the data held on media systems is purged when its life time expires and issues to do with backing up data so that resilience is attained in data availability. (2) identity management and access control which deal with ensuring only the rightful owners to the data can access it and make use of it and (3) contractual and legal issues which border on ownership and usage parameters of the cloud systems in question [61] [63].

2.4.6 Security Isn't About Hardware and Software

It must be understood that security is a process and that there is no tool that has ability to provide full-proof security for an organisation or individual as far as information security is concerned [45] [46]. All security products are only as secure as the people who configure and maintain them. All the individuals who purchase security systems must equally be given training time and senior management of that organisation must ensure that their staff have met this training time by running performance reviews. Sufficient review must be taken by the management of an organisation to verify that the user team has had sufficient training in the security aspects of the installed security devices. Security must not be left only to the individuals who install and run the security systems in an organisation, all individuals must

participate in ensuring that their organisation is safely operating under the agreed standards. Security must be seen as an all-round function of everyone and not only ICT security personnel [64].

2.4.7 The Bad Guys Are Very Sophisticated

It must be understood that hackers are everywhere, and they are bent on infiltrating computing systems for their benefit. This benefit may not be obviously known to the victims of attack but are known to the attacker. Hackers nowadays group into massive organisations that plan and have intention of attack. These organisations which have huge resources are capable of employing well trained individuals that can attack an attack and bring it down in terms of computing resources. Todays' organisations primarily run their affairs using computers that are networked and an attack from a hacking organisation can greatly compromise that organisation's performance. It must then be realised that attackers or hackers have become sophisticated and the victim organisations must equally equip themselves in terms of security response by setting up response teams and employing well trained individuals that can respond to these attacks [52].

2.4.8 Security is a Drain on Resources

The conflicting language between ICT people and others working for the same organisation often creates a difficulty in translating a security need by ICT staff into an organisation requirement. The barrier in language is created by technical jargon. Organisations also require that a purchase or an investment is supported by a business case, this then means that an ICT security infrastructure reduced to paper requirements and this may imply an understanding of what is needed may be lost through written statements. The fact that security of ICT system cannot be guaranteed. This culture often leads to the impression that security is a drain on organisational resources. Management will often in such a situation view security as a necessary evil and purchase what they feel is right for the organisation. This may lead to an under purchase of the required security systems. Worse still a purchase of ICT security systems will not reward an organisation with monetary profit when compared to a purchase of a sales delivery van that quickly yields monetary income for an organisation. With such views it becomes difficult to secure an organisation and this view provides another obstacle to securing an organisation. It is perhaps ideal for management to consider training general

management staff in ICT applications and systems to counter this culture. This training ultimately would provide for a cost-benefit implementation of security systems [46] [65] [43].

Once an understanding of the obstacles to the information security of an organisation is made, an organisation is then ready to build a secure infrastructure for itself in order to securely store biometric data.

2.5 Evaluation of Civil Data Risks and Threats

Before any security measure can be undertaken it is critical for every organisation to understand the nature of the risks or risks that may affect its operations. In doing so an approach to understanding risks must be undertaken [66].

2.5.1 Understanding Risks and Threats targeted Towards ICT Systems

Two approaches are available in trying to evaluate assets held by an organisation such as computer servers and biometric data that requires security. The first approach normally recognised as the **infrastructure model** attempts to identify organisational assets and allocates security resources based on the value of each asset. The second approach normally recognised as **business model threats** attempts to evaluate the threats postured to an organisation and its data [67].

2.5.2 Infrastructure Model

In this dimension of threat analysis, an identification of risks based on an organization's infrastructure model is made. The likely threats against the infrastructure of the organisation are carefully tabulated and scored so as to understand their likely impact on each asset. Assets can be handheld devices and other computing resources that employees use for their organisational work. Organisations that may have a lot of resources interconnecting may have more risks identified than an organisation that does NOT have a heavy investment in ICT systems [68].

2.5.3 Business Model Threats

In this dimension, an understanding of the general threats that may affect a business or an industry is made. These threats or risks are then carefully understood to understand their impact should they ever surface. This analysis will extend to some form of investigation so that an understanding of possible enemies against the business is made. A histology of threats may be made as well. The key is to have a generalized view of the possible threats that may affect an organisation from possible enemies and generally what sort of threats are present and active in such businesses. Two subdivisions of this analysis yields the following further angles [67]:

i. Industry based threats and

ii. Global threats.

2.5.4 Industry Based Threats

Investopedia defines an industry as *"A classification that refers to a group of companies that are related in terms of their primary business activities",* [69]. Michael Porter alleges that there are similar forces at play against or on any industry in the competitive world [70]. A conclusion can then be drawn that organisations that form a particular industry have a more dedicated effort of attack than others. An example of this can be financial institutions [71]. It then becomes important to identify threats common in such industries by way of industry-specific trade groups or similar events in which businesses can share information regarding attacks [72] [43].

2.5.5 Global Threats

It is necessary to acknowledge that a threat occurring in one area of the globe may soon attack an organisation on the other side of the globe. Recent cases of Ransomware attacks confirm this [50]. Because of this kind of attack it is then critical for any organisation to understand how one attack may globally find and compromise that organisation [67] [73].

Once the threats have been realised, an organisation has options of dealing with those threats in the following ways:

i. Ignore the risk: the organisation will elect NOT to implement any measures to manage the risk [66].

ii. Avoid the risk: in this arena an organisation will implement measures that prevent the occurrence of the risk(s) in question [66].

iii. Accept the risk: An organisation may choose this route in the event that no viable countermeasure exist to ameliorate the risk. This option may also be taken if the proposed countermeasure may be more expensive than suffering the risk impact. Sufficient information should have been collected by the organisation during its evaluation on the risk and its effects before this choice is picked [74].

iv. Transfer the risk: in this avenue the impact of the risk (should it occur) is made to fall on a party, other than the organization. The common option here is to purchase insurance of some form from a third party. The insurance company then agrees to take on the risk [75].

v. Mitigate the risk: this avenue, if adopted allows an organisation to engage its resources in such a way that the impact of the risks identified should they occur are reduced [66].

2.5.6 Common Misconceptions

Irrespective of the type of organisation one is observing, it must be known that as long as that organisation utilizes computer systems and computer networks, personal data is most likely to be retained on one the computing resources available in that organisation. This information is of vital importance to a cyber-attacker because chances that personal data in the region of financial details may exist on the computer systems. An attacker may have a keen interest in such data. This data may be stolen for sale to organisations that use it in the generation of identity cards or generation of credit cards and others [58] [76] [77] [78]. A misconception that is held by organisations that use computing resources in certain industries is that their computer systems are not targeted for attack from anyone. Bishop et al. [79] urges an understanding of psychological factors affecting individuals in the management of insider threats. Individuals may attack an organisation they work for in terms of stealing information or disclosure of information because of *schandenfreude*. Organisations must not have a

misconception that no one is out to attack their organisation [79].

2.5.7 IT Security Training

In order to ensure that staff within an organisation always execute their duties according to organisational policy it is important to ensure that staff get the right training. Training delivers the right interventions, right skill and attitude to an employee within an organisation and guarantees that that employee executes discharges functions according to the wishes of their organisation this is true even for the security aspects of an organisation. It is important that staff are given the right training to ensure that they are able to cope with the changes in technologies and the ever changing information security that arise. Organisations can identify training programmes that define security aspects for IT systems that are ideal for an organisation and ensure staff are given these trainings. Among the world-renowned ICT Security training programmes include programmes like the COBIT programmes and CISSP programmes. Organisations can adopt such programmes and ensure staff receive such training. Acquiring professional ICT security training is recommended here [67] [43] [80].

2.5.8 Unconventional Security Techniques

Threats that affect an organisation must not be seen as only coming from outside an organisation. It is important to realise that threats can come from employees within an organisation who are not bent on harming an organisation [46]. A threat may become a reality if an employee for instance lost a work computing resource such as a computer (stolen, say, which is pre-configured to access the company network). This lost computing resource may introduce a threat into an organisation should be it be found or be stolen a by an attacker who uses it to launch an attack on the organisation. Organisations, therefore, must think '*outside the box*' in realising that threats can come from those areas one least expects. A USB flush-drive innocently used by an employee to transport information to a home computer in the effort of carrying work home may result into an introduction of a malware from home to work. Threats to computing resources can come from variables that are unknown to the employee, threats may come from technologies such as baseband for instance [81] [43].

2.5.9 Security Culture

"Broadly, social heritage of a group (organized community or society). It is a pattern of responses discovered, developed, or invented during the group's history of handling problems which arise from interactions among its members, and between them and their environment"

[82]. From the definition it can be understood that culture is a *'pattern of responses'* that have been discovered. It then follows that an organisation from its past and immediate interactions with threats to its ICT resources must grow a culture pattern that ensures that the individuals or employees can adequately respond to threats that present themselves. Employees are key to the success of the organisations they work for; therefore, it is important to ensure that the employees can adequately understand the threats that may come into an organisation from either the insider or outsider regime. This then means that it is important, therefore, that a culture of continuous knowledge upgrade towards the understanding of ICT threats is inculcated in the organisation. This culture must be internalised by all organisational staff and remedial assessments must be undertaken to ensure staff are internalising such a culture. A fully internalised culture may help avert the probability of ICT risks from harming an organisation [83].

2.5.10 Understand OS and Application Strength

Operating systems are essentially built with security features that are meant to ensure that computer application software and other programs to operate within pre-set limits without causing interference to other applications. Operations outside set parameters must be stopped. Security features within an operating system may be activated and configured to ensure that the computing resources and their related network are protected. Individuals and organisations must ensure these security features are activated and well configured to achieve this desired security. Among other security features to configure are performing regular OS patch updates, Installing updated antivirus engines and software, scrutinizing all incoming and outgoing network traffic through a firewall and creating secure accounts with required privileges only [84] [68] [46] [45].

2.5.11 Systems Surveillance

In order for any security specification to work effectively, an organisation or individual that is utilising such a service must continuously monitor or keep surveillance over such a system. Keeping surveillance refers to active monitoring all areas that may be understood as potential attack points for an attacker or points that have been identified as weak points or points that have had an attack presented on them. Keeping an eye on such installations ensures that once as attack becomes present it becomes easy to prevent or mitigate. A log or attack points and potential attack points must be made after a careful systems risk assessment. This log must be kept and updated when new attacks are identified. This log must be used to monitor the system

security. Logs such as this must be used in conjunction with systems audit to ensure all relevant points that require security are dealt with. This should help in securing an organisation or individual's systems as far as computing resources and networks is concerned [43] [47].

2.5.12 Third Party Audits

To ensure an organisation's computing resource is properly secured, it is apparent that an organisation hires the services of a third party audit security. A third party audit security company brings in a second eye on the security aspects of an organisation. This difference in perspective allows for identification of threats and possible threats that could have been overlooked or not identified by an organisation's security team [85] [43].

2.5.13 Apply Basic Security

Basic security management must not be overlooked by systems administrators. Things such as training users on the use of networks properly, use of strong passwords, ensuring that passwords are not written on papers and left anyhow within an organisation, securing USB flash drives and others must be continuously preached to the users in the organisations. Basic security elements must be practiced on a daily basis, this helps an organisation refine its entire approach to security in the organisation. Users in organisations must from time to time be given workshops on security in the use of computing resources. If well implemented this may help an organisation meet its security requirements [43]. Certain individuals have a tendency to write their computer or server passwords on paper. This practice may lead to data theft as the paper may go missing or an adversary may steal it with the hope of stealing information from the computer servers. The error here is the use of paper to retain credential data. Individuals or employees must be trained NOT to use paper for storage of sensitive data such as passwords. Management of paper by restricting an organisation's activities to paperless or close to this must be one way in which an organisation can implement security measures to protect itself from attackers. Implementing guiding policies such as shredding of paper must be encouraged [86] [45] [46] [51].

2.5.14 Update When Available

Systems that are installed normally have updates in as far as security is concerned. These updates are responses to the new and emerging threats on the cyber market. It is critical for an organisation to update and install these patches to ensure that its systems are secured up

to the current available security. This ensures that all new and emerging threats would be stopped from successfully compromising an organisation's computing resources and related networks [87] [88] [47].

2.6 Authentication

Authentication is a process that establishes an entity in a communication process (or any activity) and binds it to that communication process (or any activity) [46] [65]. Basic forms of authentication can be achieved via the use of passwords and pins (personal identity numbers). Due to the advancement in computing technologies, both password and pin authentication can be bypassed by an unauthorised third party via tools which can either exhume password or pin hashes from a computing resource or use software vulnerabilities to bypass them [52]. Due to this threat, an extended form of authentication exists called a Multi-Factor Authentication (MFA). This type of authentication uses more than one piece of datum or technological tool to identify and bind an entity to a transaction [46]. Agreeing more than one independent factor escalates the effort of providing false credentials. A multi-factor authentication pledges an advanced protection level by extending the single authentication factor. A Two-Factor Authentication (2FA) uses two items of data to identify and bind an entity to a transaction [89].

In a biometric setting, a retina or a facial scan and password or username can be used to bind an entity to a transaction. In such a setting an individual would provide a two-fold technique for noticeable verification. The goal of a 2FA is to make a dual hindrance and make it more problematic for an unapproved individual to get an unauthorised access to a resource [9].

2.6.1 Person Identity, Biometrics & Authentication

Person identification requires recognition of humans by using past captured data about that person (say a photo or finger print) or authentication by using some aspect about that person that confirms their identity (say a signature) [90].

2.6.2 Practical Elements of Identification Features in Man

Several features about man may be used to identify that person. Among them include Name, Sex, Birth place, Tribe and NRC number [46].

2.7 Biometrics

Biometrics is about measuring unique personal features such as a subject's voice, fingerprint,

hand geometry, feet geometry, or iris (includes even blind people [91])storing them and later on retrieving them so as to use them to provide identification or authentication of the owner. It has the potential to identify and separate individuals with a high degree of assurance, thus providing a foundation for trust [92] [93].

The use of biometric data presents with the problem of accuracy, reliability and an impeding problem of data theft. Once biometric data is enrolled into a databases or software system for later use, what matters is how accurate that information would be in re-use [93].

2.7.1 Special Population Use

A special population is generally viewed as a disadvantaged group or a disadvantaged individual. Some individuals or people might experience disadvantage due to being more sensitive or vulnerable to exposure to hazardous substances. Certain factors such as age, occupation, sex or behaviour contribute to an individual's vulnerability. These individuals or groups of people will therefore require special consideration and attention in almost all environmental settings [94] [95]. Individuals falling into the category of special population can be understood as [94]:

i. People with behavioural and emotional disturbances that can be understood as concurrent mental disorders;

ii. People with learning and intellectual disability;

iii. People with development delays or differences;

iv. People with physical disabilities and

v. People that have circumstances or conditions that require special attention like individuals with medical comorbidities (presence of more than one disease or disorder e.g. a person suffering from a disease such as Cancer may present with anxiety).

In an event that an individual whose fingerprint or hand geometry or writing (pressure reader) biometric data is enrolled into a suitable biometric identification and authentication system suffers injury, say, through an accident, on that same

hand that is enrolled into the system, then the biometric system WILL NOT be used reliably. Identification or authentication WILL NOT be successful [41]. Individuals that have eye distortions caused by accidents or sickness but have their eye biometric data enrolled into a biometric system may not have access to the services that that system offers as the eye distortions result into a false rejection. Individuals that wear glasses may also NOT be enrolled into an iris biometric reader as refraction may play a role and impede the accuracy process of the reader [94] [96]. A voice capture biometric system may not be able to allow access to an individual should that enrolled voice have a variation. Variations in a voice can come from sickness such as a cold. A further variation may be created by an external noise source or general noise within the area that the voice recognition must occur. This noise has the capability to compromise the accuracy of the voice biometric reader [94].

2.7.2 Biometric Technology Types

Biometrics can be collected from either a physiological characteristic or a behavioural characteristic. A physiological characteristic is a relatively stable human physical feature. An example of a physiological characteristic is a fingerprint, retina iris pattern, or a hand-geometry pattern. Physiological measurements are static and non-alterable. This type of measurement is unchanging and irreversible or permanent apart for deformity caused by external significant duress such as ailment or physical injury [97]. A behavioural characteristic on the other hand attempts to resemble a person's psychological makeup. This is affected by a person's build stature and gender among others. Behavioural characteristics can be identified in activities such as speech, hand-writing speed and pressure exerted on paper when writing among others [98].

Biometrics can be classified as:

a) Static: unchanging human features can be recorded. These include things like fingerprints, hand geometry, and face structure, retina and iris patterns and
b) Dynamic: measurement of slight changing features is continuous as it is input e.g. voice, writing and keyboard response times.

Identification based on biometrics is superior and works extremely well at sorting people than most people identification systems such as a person's visual memory. [46]

Four methods of biometric authentication systems were reviewed employing both physiological and behavioural characteristics. These have been reviewed in terms of basic operation, advantage and disadvantage of implementation.

2.7.2.1 Fingerprint Authentication

Fingerprints are made up of ridge patterns on a person's fingers. These ridge patterns have capacity to uniquely distinguish and identify individuals. Fingerprint features are made up of arches, loops, and whorls. An individual fingerprint will exhibit at least one of these major features. The minor details that are collected from these fingerprint features are referred to as minutiae. Figures 2.11 and 2.12 show a finger print sample and finger print features. The authentication processes is an automated method of verifying a match among different human fingerprints [99] .

Advantages:

i. Individualistic features guarantee authentication of subject [97];

ii. Systems are relatively inexpensive to purchase and install;

iii. Longevity of life of the fingerprint pattern's individualistic feature composition guarantees long term usage [97];

iv. Once in use a subject does not have to rely on memory for passwords as fingerprint authentication will guarantee access and

v. A fingerprint identity point cannot be spoofed [45].

Disadvantages:

i. Limitation of capture is reduced to an individual finger with further limitation of capture reduced to a section or part of that finger only and not the entire finger;

ii. Susceptible to FAR (false acceptance error) whereas a wrong subject is enrolled and allowed access;

iii. Hand injury (fingers included), chemical prone jobs and labour prone activities such as brick-laying or metal fabricating present a within-person variation that makes the reading and capture of finger prints difficult and

iv. Washing with a soap detergent or submerging a finger in water for period of time (approximately 30 minutes) works as a contraceptive to finger-print scanners and this may impede the scanners from capturing or enrolling the finger prints until the finger reverts to its original form it was in during capture or enrolment [46].

Figure 2.11. Fingerprint Image Sample [107]

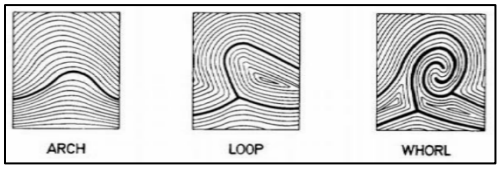


Figure 2.12. Fingerprint features [101]

2.7.2.2 Retina Authentication

This is one of the two forms of eye biometrics; the other being iris recognition. This form of biometrics is one of the most secure authentication systems in place today. The installed technology requires that an impression of a retina pattern must be taken and stored. The authentication process involves evaluating a subject's retina with a stored version (impression enrolled) of that subject's retina. Retina recognition has a low FAR (false acceptance error) as well as low rejection rates [52]. An image sample of an eye is shown in Figure 2.13.

Advantages:

i. Different even in identical twins;

ii. Highly specific with unique structure shape and limits the possibility of fake retina presentation;

iii. Longevity of structure throughout life time of subject;

iv. Wearing of glasses or contact lenses does NOT work as a contraceptive to technological accuracy and

v. High accuracy and High recognition process speed.

Disadvantages:

i. Eye injury or sickness may render this biometric system ineffective;

ii. Intrusive technology and may not be welcomed by many individuals;

iii. Lighting may affect the accuracy of the reader and

iv. Fairly expensive to acquire when compared to other systems of biometrics.

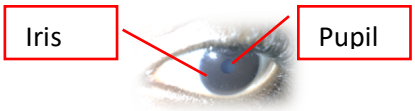


Figure 2.13. Eye Image Sample – for iris Recognition [52]

2.7.2.3 Voice Authentication

This technology allows the conversion of voice or sounds from human voice into an electrical signal that can be coded. Voice recognition software is designed to identify an individual via their unique voiceprint. Voiceprints are generated from physical characteristics of an individual's throat in conjunction with their mouth. Research indicates that no two voices are the same and therefore voice biometrics provide a rare opportunity to use one's voice to authenticate or identify individuals [100]. A sample of a voice pattern is shown in Figure 2.14.

Advantages:

i. No need for user training as users can simply speak into the voice biometric reader;

ii. Voice communications is a natural activity for human beings;

iii. Voice communications eliminates the need to learn keyboard operations (and in this way helps to bridge the gap between the able-bodied and individuals who experience restricted capabilities in hand based motion activities such as

writing). By eliminating the learning aspect, voice overcomes the need to learn how to operate some complex biometric technology's operations;

iv. It eliminates the need to be accurate in written statements as is for password based authentication and

v. Because one uses voice, the speed of operation is enhanced. People generally speak faster than they are able to write.

Disadvantages:

i. Impulse noise may affect the accuracy of the voice signal and render the system ineffective;

ii. Microphone proximity must be precise for the system to work well;

iii. A pre-recorded audio may by-pass this system;

iv. A person may speak different languages, and this may affect the accuracy of the device should that individual use a different language or dialect;

v. Certain words have a homonym characteristic, this may affect the accuracy of the device;

vi. The learning curve for the system may be long as it is trained per voice and

vii. Most voice controlled biometrics are expensive.

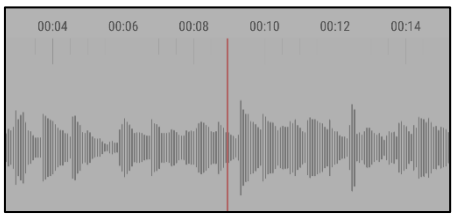


Figure 2.14. Voice Print. Adapted from [137]

2.7.2.4 Face

Facial biometrics divides into two aspects namely the face detection and face recognition programs. Face recognition extracts a face from a given image while face recognition compares a captured face against saved faces in order to match the face. The entire process is run by a series of complex algorithms. One of the options of face recognition is to select features of a face and match those features

to a face. Figure 2.15 shows a facial image sample with facial image mapping that is used to collect facial features. The facial features or dataset is normally stored in a database. In ideal situations this database must be encrypted to achieve sufficient security [101].

Advantages:

i. Non-intrusive technology and can be performed stealthily without the subject knowing, therefore, proves ideal for investigation purposes;

ii. Certain algorithms can be adjusted to scan a large scale of a population and thus this technology proves ideal in crowded environments;

iii. Ideal for person tracking and incident reporting;

iv. User friendly as far as users are concerned as no need of complex training for the subjects to be captured;

v. Can be developed and run from a basic computer camera without buying any other tools. This proves to be one of the strongest advantage and reduces the cost of this technology exponentially;

vi. Some easy to install ready to use pre-trained facial calibration tools are available. This again reduces cost of setup and

vii. Facial biometric algorithms have a within-person variation calculation that can detect aging and basic facial deformity and reduce a face to a known variable [102].

Disadvantages:

i. Certain algorithms may NOT work well on black faces;

ii. Light conditions and camera capabilities may affect the accuracy of the technology;

iii. Within-person variations may affect the accuracy levels of the technology [103] and

iv. When used for security purposes, extra equipment to provide lighting can increase cost of setup.

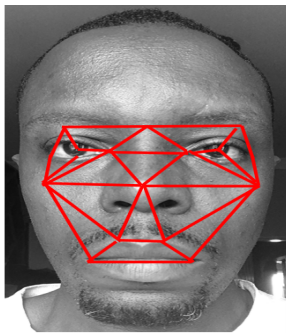


Figure 2.15. Facial map for Facial Biometrics. Adapted from [137]

2.7.3. Within-Person Variation

Human faces have been used since time immemorial in the everyday recognition and authentication of individuals. Face recognition provides a secure means by which a person can be identified.

Faces, however are faced by a problem that is difficult to solve with precision. This problem is referred to as the problem of aging [103]. Aging can be understood as a length of existence of a person (or thing). During this existence human facial appearance changes due to the process of aging. The process of aging presents with it factors such as bone growth, loss of elastic property in the facial skin and the subsequent pull of gravity on that skin. Other factors such as facial deformation are pronounced as one ages. All these factors inhibit the successful growth of, and implementation of biometric science in person identification [102]. Person variations that are due to accidents or other extenuating circumstances that create facial deformation are beyond the scope of this dissertation. Much discussion is focused on facial recognition as this forms most of the delicate data items generated due to within-person variations.

Person variations refer to the changes that present in facial appearances brought about by the factors of aging earlier highlighted [102] [103]. Figure 2.16 illustrates. The factors of variations imply that an algorithm must be found that takes into account such changes. As an individual ages so does the face adjust or get deformed. These changes must be taken into account in the development of an algorithm to read and match faces to individuals because the performance of face recognition and/or authentication systems is greatly affected by within-person variations encountered in human faces. Variations on facial appearance include injury to face, bone growth, and generally aging. Of these, aging-related variations tend to

show exceptional features that result into making the process of dealing with this type of variation a challenging task. To counter such a challenge an age-invariant recognition system must be designed [104].

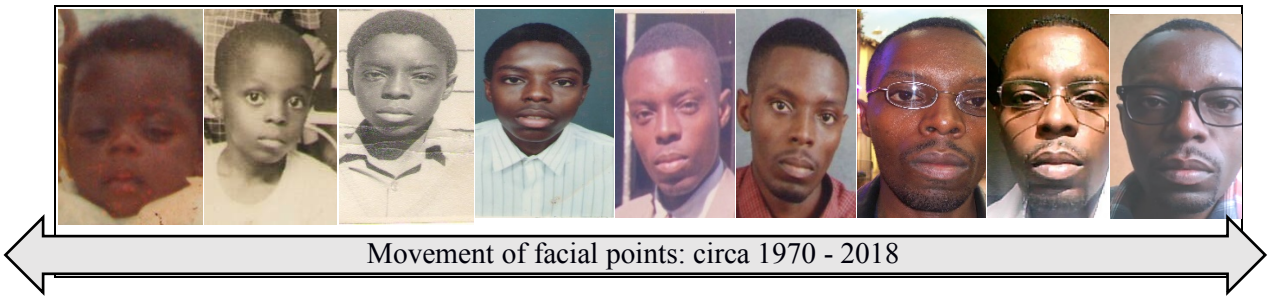


Figure 2.16. Movements of Facial Points. Adapted from [103]

Two methods of developing a facial recognition system have been proposed by Yadav et al. based on what they term as an age-invariant face recognition system. The methods are (1) facial age estimation where age estimation involves predicting the age of an individual given his/her facial image and (2) age-separated face recognition where face recognition consists of recognizing an individual given his/her age-separated images. [104]. Figure 2.17 illustrates the aged face drift images.

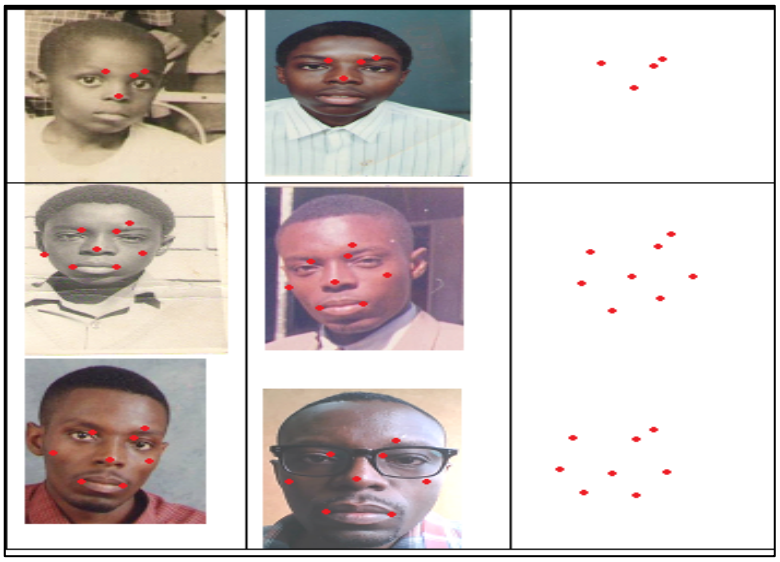


Figure 2.17. Drifts in Facial features for age separated face images. Adapted from [103]

An alternative to recognise faces deformed due to within person variations created by age is defined by Bilgin Esme & Bulent Sankur in their paper entitled "*Effects of Aging over Facial Feature Analysis and Face Recognition",* where they propose two methods called (1)

Generative Approach – where by applying a computational model that simulates the aging, an algorithm may be developed to perform a recognition and (2) Non-generative Approach – where a study of age invariant signatures is done so that a face may be recognised. The invariance in the second method is arrived at by the argument that although age deforms a face, it does not affect illumination. The argument raised by Bilgin Esme & Bulent Sankur can thus be used to generate a face recognition system in the second instance as the change in face orientation is not affected by illumination of face (the movement of points on a face due to facial expressions caused by laughter, smile, anger etc) appears to be consistent. The logic is to measure the facial drifts caused by illumination or facial appearance during an expression. These drifts are then used to identify or authenticate an individual through a facial algorithm that maps the movements and determines the face. The drift is measured by understanding the frontal trusted features. The consistency of some selected facial features is larger on two different images of the same person with different ages (see Figure 2.17). The most frontal features are selected only. These are referred to as the as frontal fiducial features. These frontal fiducial features are selected and not outer features because the features on the outer boundaries of the face tend to change promptly with head posture variations and facial actions and person mood (anger, amusement, laughing etc). Equation (1) is used to determine variation of age.

$$\cup \boldsymbol{ij} = \frac{|\boldsymbol{a_i} - \boldsymbol{a_j}|}{\boldsymbol{r_{ij}}} \qquad (1)$$

where $|ai-aj|$ is the magnitude of the vector difference between the two feature drifts *ai* and *aj* while *rij* is the distance between the corresponding feature locations and the combined potential energy of the drift map characterized by *K* feature drifts. Equation (2) is used to determine *K* feature drifts is.

$$\boldsymbol{C} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{K}} \sum_{\boldsymbol{j=i+1}}^{\boldsymbol{K}} \boldsymbol{U_{ij}} \qquad (2)$$

In this work, a conclusion is made that the lower the potential energy C, then it is more likely that the images belong to the same person [103].

From it then follows that biometrics have consistency. This consistency then ensures that a biometric feature has longevity of integrity as long as the subject is alive [96]. This consistency of a biometric feature is tied to the fact that a biometric signal is constant in time save for exogenous circumstances like injury [105] [97] [106] [107]. To achieve biometric

consistency, a match which uses a raw signal or fresh input (the biometric template or *BT*) must be collected from the signal directly at feature matching (the biometric signal or *BS*). Therefore, the biometric, *B*, is governed by *BS, BT* and *B*. Equation (3) can be used to determine stability of a biometric signal [108].

$$\llbracket BT \rrbracket\_s = f(B) \qquad (3)$$

Pregnant women may encounter changes to their faces caused by the pregnancy. These changes may result into severe deformation of the face and result into within-person variations that may prove challenging to identification algorithms, as such the same challenges and constraints experienced in all other cases may hold. It is then advised that facial recognition in pregnancy must be avoided and an alternative such as iris or finger print recognition may be used [109].

A conclusion can then be made that research is on-going in this area of person identification caused by within-person variations.

2.8. Security Issues in Identifications and Authentications

In his paper citing Alexander Trechsel and Kristjan Vassil from their writing, "*Internet Voting in Estonia: A Comparative Analysis of Four Elections since 2005', European University Institute, 2010"*, Professor Thad Hall raises concerns about the security of a voter's detail if electronic means are to be used to deliver an electronic vote [110]. The security in question here borders around the concerns of whether Electronic systems can be attacked through various schemes such as denial of service, spoofing, viruses, and man-in-the-middle efforts among others.

The cryptographic property of a biometric piece of data once collected from an individual cannot be matched by any other piece of biometric data collected from a different person other than the one who provided it initially [111]. This impossibility extends to biometric data in the form of hand geometry, fingerprint or eye data [112] [105]. This feature of a biometric datum is enough to allay fears of Identity theft. Secondly once a biometric datum is retrieved from an individual, cryptographic means can be used to encipher the datum; this guarantees that an encrypted datum is non-understandable even if it is stolen. An enciphered or encrypted biometric datum is in a form that a third party cannot understand or decipher [46]. The

physical security measures of ensuring actual theft of biometric data lies with the institution charged with the responsibility of capturing these data pieces.

In the "*Analysis of an Electronic Voting System"* paper by Tadayoshi Kohno, a fear is raised about a possibility of a man in the middle attack which can result into the theft of electronic data as it propagates [113]. Though this is a true possibility, a fully secured crypto system can be developed that can utilize a MAC (message authentication code). A MAC would counter the issues related to live data theft and subsequent tempering of the same by applying an image resistance property [46].

2.9 Cryptography

Cryptography focuses on developing and studying mechanism that use science and math principles to deliver security mechanisms. Its main aim is to hide or conceal messages so that confidentiality can be achieved [114].

The word 'Cryptography' combines two Greek words namely:

(i.) 'Krypto' meaning hidden and (ii.) 'Graphene' meaning writing [115].

Cryptography aims to deliver five (5) security services to Information Security as explained [46] [45] [65]:

i. *Confidentiality:* This security service aims to give an assurance that data cannot be viewed by an unauthorised user. This service may be referred to as *secrecy*. Most cryptographic applications provide the secrecy service.

ii. *Data integrity:* This security service aims to ensure that data cannot be altered in an unauthorised (this also includes accidental) manner. This assurance applies from the data creation point, transmission or storage by an authorised user. The main principle in data integrity is NOT the *prevention* of alteration of data, but a means for *detecting* whether data has been manipulated in an unauthorised way.

iii. *Data origin authentication:* This security service aims to provide the assurance that a given entity was the *original source* of received data. If a technique provides data origin authentication that some data came from source A (or Tx), for instance, then this means that the receiver B (or Rx) can be sure that the data did originally

come from source A at some time in the past. Data origin authentication is sometimes referred to as *message authentication* since it is primarily concerned with the authentication of the data (message) and not who was communicating in a transmission process at the time the data was received.

iv. *Non-repudiation:* This security service aims to provide assurance that an entity cannot deny a previous commitment or action. Non-repudiation is the assurance that the original source of some data cannot deny *to a third party* that this is the case. Non-repudiation is a property that is most desirable in situations where there is the potential for a dispute to arise over the exchange of data.

v. *Entity authentication:* This security service is the assurance that a given entity is involved *and currently active* in a communication session. If a technique provides entity authentication of source A (or Tx), for instance, then this means that by applying the technique we can be sure that source A is really engaging in a communication with a given party in 'real time'.

Cryptography is implemented using cryptographic primitives. A cryptographic primitive is a cryptographic process that provides a number of specified security services. A particular specification of a cryptographic primitive is called a cryptographic algorithm. Cryptographic primitives are enclosed within cryptosystems (or cryptographic systems). A cryptographic system may use a key to either conceal or reveal a hidden message. The hidden message is called a ciphertext while its inverse is called plaintext [116]. The cryptographic key may take one of two forms or both as follows:

A] Encryption key: value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to conceal a message. The receiver may know the encryption key. Any attacker MAY KNOW the encryption key [116].

B] Decryption key is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to reveal the plaintext. Any attacker MUST NOT KNOW the decryption key [65].

A cryptosystem is a general term referring to a set of cryptographic primitives used to provide specific information security services.

Two types of cryptosystems exist namely (i) Symmetric and (ii) Asymmetric [46].

In symmetric cryptosystems the decryption key is easily obtained from the encryption key and both may be the same [45].

In asymmetric cryptosystems it is practically impossible to determine the decryption key from the encryption key. In this case the encryption key and the decryption key are always different [46] [105].

For the purposes of this study the term biometric cryptography shall be taken to mean the capturing of a certain aspect of human attribute (physiological or biological) storing this aspect in an encrypted manner and then later when needed retrieving this human aspect of data and using it to confirm the owners' identity.

Human aspect data that may captured include [46]:

i. Eye structure;
ii. Finger print statistic;
iii. Voice statistic and
iv. Tooth structure.

2.9.1 Need for Cryptography

2.9.1.1 Binding Person Identity with Cryptography

Microsoft Encarta defines the word "bind" as *"to tie something firmly to something else by winding a cord tightly and repeatedly around both things"* [117]. From this definition two factors come to light namely:

a) To ensure either party to a bind are inseparable and
b) To ensure either party cannot escape the tie.

Following in on this, it would be prudent for an identification system to perform these activities in identification of an individual. It follows also that an identification system should NOT be easily escaped, or an individual cannot deny that he or she is

the one being identified. With biometric identification all these elements are possible. Human features such as hand geometry, retina and finger prints do not change. These elements can be used to bind an individual to his or her identity.

2.9.1.2 Security Service Delivery

A security service is a detailed security objective that an organization/ individual attempts to achieve [46]. The preceding section (2.9 Cryptography) highlights these security services.

Cryptography involves techniques of transmission or storage of data in such a way that only those it is intended for can retrieve it from a medium of either transmission or storage [46].

Cryptography involves many methods, among them is combining words, converting letters to other letters or digits or capturing human attribute data such as finger prints, eye structure and converting them into an unintelligible format i.e. non-understandable to a third party without a decryption key. Cryptographic Primitives which are computing procedures defining procedural activity are devised to execute cryptography on ICT devices [115] [116] [45] [46].

The converted message is referred to as a Ciphertext [116] (encrypted message) while its inverse is called plaintext.

An encrypted message requires a key for it to be retrieved. A key declares to an encryption primitive the reversal procedure of a ciphertext to plaintext. Without a key it is difficult to recover the plaintext [116].

A strong combination of biometrics and cryptography might, for example, have the potential to link a user with a digital signature she/ he created with a high level of assurance [118] [119].Cryptography can then be said to be a much needed tool to secure a message in transit or not.

2.10 Biometrics and the Law

The technological reality of biometrics places a drive on individuals, organisations and governments to explore further what is required for safeguarding the basic human rights of privacy and to ensure the ideal results for society. The growing number of conceivable biometric applications generates unforeseen risks and calls for better and additional security

to protect the biometric subjects whose biometric data is kept or used by these biometric systems. An examination of the law and policy concerns of biometric applications from a privacy viewpoint must be undertaken and this makes a good point to start [120].

To give an understanding of the issues involved in biometrics, biometric systems and the law, the discussion divides into the European perspective, American perspective, the trans-border biometric perspective, the UK perspective and finally the Zambian perspective. This discussion on biometric data and biometric systems examines only the privacy aspects that biometric data and biometric systems introduce.

2.10.1 Biometrics and Privacy

The initial argument to make is to establish whether biometric data is personal data or that it is just plain raw data. A need to establish this is important as privacy is the right of an individual to control the use and dissemination of information that relates to that individual in as far as that individual deems that information as NOT public information that can be accessible in public domain. Holistically, privacy can be understood as a need that an individual has to want to be left alone or not to have their life unreasonably interfered with by others [12].

Issues of privacy must be established clearly when dealing with biometrics because after all biometric data is data about an individual.

2.10.2 The European Union Perspective

The European Commission states that an equality exists between *'...personal data' and any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Raw biometrical images of a person, including templates derived from raw biometrical images, are personal data…"* [121] [120]. Within the European Union, a law referred to as GDPR (General Data Protection of 2016) fines individuals and organisations for use of biometric data classified as personal data if that data is used without the express consent of the owner. Facebook has had to pay huge fines exceeding £500 thousand in breach of use and export of personal biometric data of about 87 million people. This data involved images and other personal data such as birth details,

phone numbers among others that was harvested by third-party applications to organisations that analyse such data for their clients in order to build market preferred products [122]. In considering this argument, a conclusion can then be arrived at that all forms of biometric data as far as Europe is concerned is personal data and as such care must be employed to ensure that it is kept securely.

2.10.3 The American Perspective

In the USA, a prominent law developed in Illinois referred to as Biometric Information Privacy Act (BIPA) supervises the privacy aspects of biometric data [123]. BIPA can be examined as follows:

A definition of what is termed as a *"biometric identifier"* is given which governs how the rest of the law applies to biometric identifiers. In BIPA a biometric identifier refers to a retina or iris scan, fingerprint, voiceprint, or scan of a hand or face geometry. In this definition an exemption is given to things like photographs, writing samples, demographic data, and physical descriptions [123]. The legal systems in the USA through its courts however have re-interpreted the BIPA to arrive at the understanding that [123]:

a. *"A photograph can be converted in to a "scan of ...X... face geometry" if a piece of software uses the measurements and structure of a face to uniquely code or identify it" where X is the name of the subject;*

b. *"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual";*

c. *"Any private entity" that collects, captures, or obtains a person's biometric identifier or biometric information must first obtain the subject's consent through a "written release."*

d. *"... the entity must provide notice about its purpose for collecting, storing, and using the information, and must post a publicly available retention and destruction schedule. And the entity may not sell the biometric data (though it can re-disclose the data with consent, as long as it doesn't "profit" from the disclosure).*

The BIPA further provides for monetary compensation to an individual who is the subject of

the biometric data should these statutes be violated [123]. A sound conclusion from the BIPA can be made that biometric information is indeed person identifying information and it is personal data. Following this argument, all laws referring to personal data can then be applied. The implication of BIPA is that biometric algorithms that are used to enrol and match an individual to their pre-enrolled datum must and can only do so if a valid consent is acquired from the subject prior to biometric capture.

2.10.4 The Trans-Border Biometric Perspective

In assessing the deployment of biometric systems across different countries when individuals' cross from one country to another, it is imperative that integration of biometric systems must be made in a comprehensive legal framework that requires greater transparency, accountability and supervision [124]. Diaz in her writing; *"Legal Challenges of Biometric Immigration Control Systems",* argues that countries which deploy biometric systems do so without considering human issues; their focus is only on technical issues. It is necessary that all countries that deploy biometric systems must utilise such systems to collect person behavioural or physiological data with the full knowledge of the subject. An individual must be made aware of the intent to collect the biometric data and its intended use [124]. International and domestic policy must be made to cover aspects of immigration biometric use. Diaz focuses her study on Australia, Mexico, New Zealand and Spain in understanding the legal issues of trans-border biometric information flows. In this work, Diaz, further states that public debate and opinion are critical in installation of biometric systems and that people whose biometric data has been extracted from, must have right to ownership of that biometric data. It is further argued in this work that due to differing terminologies and technical approach in the harvesting of biometric data; determining statistical data related to the use of biometrics proves to be difficult [124]. It is then important that trans-border biometrics must be carried out within a defined international standard that can supervise cross border biometric capture and use [124].

2.10.5 The United Kingdom Perspective

The United Kingdom has defined several laws that mitigate privacy and civil problems that biometric use introduce. Among these laws are the General Laws that can be broadly used to provide legality over the use of biometrics and biometric systems; Human rights and criminal laws that govern the rights and privileges of an individual in as far as their biometric data is used.

2.10.5.1 Data Protection Act 2018

This is part of the UK laws that generally cover data protection. The Act applies to biometric data in the same way as to any other personal data. The basic guide to the Data Protection Act is that the data about a subject (person whose biometric data has been collected into a biometric system) must be fairly and lawfully processed; must be processed for intended purpose(s); must be adequate, relevant and must not be excessive. This personal data must be accurate and kept accurate, must not be kept longer than needed and must be processed in line with rights of the subject. The personal data must NOT be transferred to countries outside the European Economic Area without adequate protection [125] [92].

2.10.5.2 Human Rights Act 1998

Apart from a legal circumstance that requires the law enforcement agencies to interfere with an individual's privacy, every person within The United Kingdom has a right to have his/her private life respected and not intruded into. The interference by law enforcement implies investigations into crimes and related activities. The right to privacy as covered by the Human Rights Act 1998 extends to biometric data and biometric systems from collection to storage of the same data. Article 8 of the Human rights Act prescribes the foregoing [126] [92].

2.10.5.3 Fingerprinting

2.10.5.4 Police and Criminal Evidence Act 1984

Part V and Schedule 2A of this Act allows the police to collect and retain all recorded fingerprints. This collection also encompasses those individuals not convicted of any crime. Fingerprints can be collected without consent of the individual [42] [92].

2.10.5.5 Criminal Justice and Police Act 2001

This Act allows police to retain copies of fingerprints. An extension of this act is that it allows the police to recapture fingerprints so as to ensure the quality of the record is improved [92] [127].

2.10.5.6 Immigration and Asylum Act 1999

This law gives Law Enforcement agencies to collect fingerprints from any individual

who asserts that he/she is claiming refuge or asylum within the UK. This collection extends to individuals who also claim other categories such as work and entrepreneurial ventures. The fingerprints must however be purged if that individual is given permanent stay within the UK. The file retention period is 10 years. The law extends to the immigration service in that they are required by law to share fingerprint data collected from asylum seekers with the police and other law enforcement agencies in relation to offences committed under the Act [128] [92].

2.10.6 The Zambian Perspective

In Zambia, the country's Electronic Communications and Transactions Act of 2009 which governs use of electronic systems and ICT read together with the country's National ICT policy adopted in April 2006 do not cover issues of biometrics [129] [130]. The Government of Zambia has, however, made a pronouncement to amend several laws that will directly affect the posture of the ECTA 2009 and a further introduction of several laws that may affect biometrics. These laws are yet to be effected and published [131].

A conclusion from this discussion is that biometric data and biometric systems must be used within the permissible law. It is an established fact that biometrics affect privacy and as such must be used not to injure the privacy of individuals or subjects whose biometric data has been collected. The author also holds the view that biometric data is personal data as established from the various legal positions presented. The author also holds the view that international agreements are needed to guide all countries in the collection and exchange of biometric data. Perhaps it would be ideal for all countries to define a single database that would hold this biometric data and allow member countries to access it as and when need arises.

2.11 ISO Standards

ISO is an Organisation that generates documentation that ensures that when used correctly, then a production of a sort can be governed to produce a materiel that has consistency in integrity even with multiple production. In other words, ISO generates standards. ISO membership is within the region of over 160 countries. ISO has published over 20,000 standards. ISO was founded on 23 February 1947 and is headquartered in Geneva, Switzerland, [132].

In the management of civil data concerning birth registration the United Nations through the WHO working in conjunction with the World Bank is the standards developer [24]. The management of civil data must however be supervised through a standard that ensures that all collected information is secured as this information will pertain to an individual. Information contained in a civil system is essentially PII. To be able to achieve this security need, ISO standards are used. Since the author is of a view that a biometric model is developed for civil systems, an appropriate ISO standard that can supervise biometric data must be used for the management of this biometric data. The IEC (International Electroctechnical Commission) is a body that ensures international standards conformity and performs assessment for all fields of electrotechnology. ISO and IEC work in conjunction to develop and enforce international standards [133] [134]. IEC publications guide nations on standardization [133].

Appropriate standards that have been determined to fit these two requirements are the ISO 27001 and the ISO 24745.

2.12 Applicable Standards to Biometric Data

2.12.1 ISO 27001

ISO 27001 (also referred to as ISO/IEC 27001 is the international standard describing the best practice for an Information Security Management System (ISMS). An ISMS is a system of processes, documents & documentation, technology and people that help to achieve, monitor, audit and develop an organization's information security [134].

By applying ISO 27001 an Organisation can perform a risk assessment tailored to ISMS that can be used to appropriately secure an Organisation or country's data and ICT systems. Biometric data, QR code data and electronic civil data is used on ICT systems and networked computing resources; this entails that ISO 27001 must be used to safely secure this information and systems in use from data attacks.

2.12.1.1 Benefits of ISO 27001 implementation

Once implemented it is envisaged that the following benefits will accrue to an Organisation or nation:

i. Protection of data;
ii. Enhancement of reputation as the use of ISO 27001 is internationally recognized;
iii. Compliance with legal and regulatory frameworks as regulators normally implement international standards;

iv. Improves structures of data as the data is made to fit into international standards for data structures;

v. Reduces frequent audits as ISO 27001 gives an indication of international security effectiveness and

vi. Introduces independence in the development of opinion towards an organization's security posture due to the fact that external auditors review ISMS at different levels to establish controls are operational as predicted [134].

2.12.2 ISO 24745

This standard provides a guide on the protection of biometric information under several information security requirements in particular the need for confidentiality, integrity and renewability or revocability during the storage and transfer of biometric data. ISO 24745 is equally used to ensure secure and privacy-compliant management and processing of biometric information [112] [111]. Further material on ISO 24745 is covered in section 4.6.3).

Biometric data is data that directly relates to the identification of an individual and in this regard care of the highest must be taken to ensure that such data does not fall into the hands of fraudsters who can use it for purposes of identification theft and others. To ensure such safety is in place it is advisable that ISO 24745 is used by all organizations or countries that are implementing biometric systems.

Due to the fact that the author is proposing a model based on biometrics, this ISO 24745 must be used in conjunction with ISO 27001 to ensure safe usage and delivery of all civil biometric data that the system shall create and utilize. The major benefit of applying the ISO 24745 standard is provision of security to biometric data at both storage and transmission.

2.13 QR Code

A typical QR code is shown in Figure 2.18

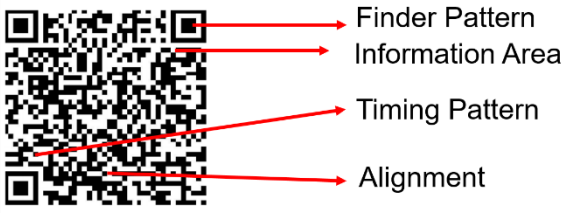


Figure 2.18. Sample QR Code. Adapted from [135]

As shown in Figure 2.18, a QR Code is a machine readable imprint made out of an array of black and white squares that normally embed certain information within the print. QR Codes were developed by a Japanese company called Denso Wave for purposes of tracking manufacturing processes. QR Codes however, provide an opportunity to authenticate as well as identify an entity. In this way QR Codes may be used as an added security feature especially in logging into networks and as a form of identifying or authenticating an individual to an entity. Networks or computer databases such as civil databases may be designed to read QR Codes, verify the data and offer, identify, authenticate or deny access to an entity. Because QR Code information is non-human readable, this provides a basic form of information hiding in plain sight (encryption). This hidden information can then be transmitted. When used with geo-tagging, QR Codes can be used to determine a location status of an entity [135] [136].

QR Codes can be mapped to contain any sort of information that a user may intend to place inside the imprint.

2.14 Summary of Related Works

Rupinder and Nana compared various biometric systems by defining their advantages and disadvantages. This work's comparison is limited to Face, Iris, Fingerprint, Finger Vein, Lips, voice. The comparison criteria defined in this work is restricted to accuracy, size of template, cost, security level, and long term stability of the biometric system they discuss. The work however does not recommend ideal biometric system [137].

Viola and Jones presented a fast (image) object detection method that describes a machine learning approach for visual object detection. The approach is different from other works due to 3 factors: [a] use of image representation called the "Integral Image" which allows a detector to compute images quickly, [b] Introduction of AdaBoost; a learning algorithm which uses weak and strong classifiers and [c] A method for combining weak classifiers into a strong classifier by generating positive and non-positive images based on face or no face analysis. The finding in this work is that detection works. The gap in this work is that the method is not incorporated into a programming utility [138].

Lienhart et at. extended the Paul-Viola AdaBoost algorithm by addition of rotated haar-like features. These additions enriched the simple features used by Paul Viola and Michael Jones and can also be calculated efficiently and improve the false rejection or false acceptance rate by an average of 10%. Three detection boost algorithms (Discrete, Real and Gentle Adaboost)

and weak classifiers are compared on the detection performance and computational complexity. The major finding in this work is that that Gentle Adaboost classifiers outperform Discrete Adaboost. The work however limits the facial dataset (bases) to a single dataset [139].

Christy et al. discussed issues of implementation of a two-factor authentication method by using alphanumeric Password and graphical Password as means for authentication. A description of the two factor Authentication (2FA) system design and design implementation was made in this work. The major findings were that 2FA adds an extra layer of security. This work does not discuss authentication of biometrics and QR Codes [9].

Onywoki and Opiyo discussed an approach to develop a framework for the adoption of biometric ATMs in the Kenyan banking sector. This work presented a developed framework which was applied to study factors influencing adoption of biometric ATM authentication and validated the developed conceptual framework. The study established that performance expectancy, effort expectancy, social influence and user privacy were key determinants for biometric ATMs acceptance, adoption and usage. Further, the study determined that age, gender and experience were moderating factors on effort expectancy with experience further moderating performance expectancy, effort expectancy, social influence and user privacy. The work is limited to ATM biometric authentication [140].

2.15 Summary

The foregoing chapter has highlighted aspects of civil data, civil registration and why civil data is needed and used by individuals and countries. Elements of problems that exist in civil registration and management have been highlighted and comparatively how civil data is collected in countries studied have been brought out. A discussion on biometrics, encryption, QR Codes and authentication has been presented and a presentation of countries under study which have utilised biometric systems for their civil data management has been made. The chapter has also cursorily look at related works concerning biometrics, civil data, algorithms plus frameworks in use concerning biometrics and their management.

CHAPTER 3

METHODOLOGY

3.1 Introduction

This chapter discusses the resources and methods that were used in this research study. The chapter is arranged around what is referred to as a baseline study. The baseline study itself includes: mixed methods research methodology, descriptive research design, target group, sample size, data collection tools, data analysis, ethical considerations, limitation of the study and presentation of findings. This chapter also has discussed issues concerning the system design methodology in the following: current birth business processes in the birth civil registration for both urban and rural environments, proposed model for birth civil registration processes; overall business process flow for the proposed model and areas of use. The chapter has further been written to explain issues to do with the system architecture which includes: system architecture, system requirement specifications, system modelling and design.

The chapter is written to explain the methodology that was utilized to conduct the baseline study coupled with the methodology used to design the models and therefore implement the prototype.

3.2 Baseline Study

3.2.1 Mixed Methods Research Methodology

The baseline study was used in order to investigate the awareness levels and understanding of biometrics among individuals and organisations and to determine if a biometric standard that defines use and management of biometrics in Zambia is in use. Additionally, the use of the baseline study was to establish if organisations which utilise biometrics for one function or another do so within a framework that is defined by government regulators of ICTs. As a result, the study used a mixed methods research methodology to analyse the data from the respondents.

A mixed methods research study can be understood as a type of research which encompasses the use of multiple approaches or methods of design, data collection or data analysis within a

single program of study (e.g. both qualitative and quantitative research), in order to incorporate the dissimilar approaches or methods occurring during the program of study, and not just at its concluding point [141]. Mixed methods designs are used to provide pragmatic advantages when exploring complex research questions.
Consequently, the baseline study used qualitative data to extend understanding of survey responses while the statistical analysis was done to provide detailed assessment of patterns of responses.

The investigative process of merging both qualitative and field survey data by developing into quantities qualitative responses consumes a lot of time consuming and is also costly in terms of resource such that researchers may not be able to yield a good result of the study due to certain compromises especially on sample sizes and ultimately limit time spent on filed data collection. Due to this characteristic, research study designs based on mixed methods have become most suitable for studies that do not require either extensive, deep analysis of qualitative data or data variables from multiple sources [142].

Mixed methods approach to research when used provides sufficient help to a researcher to incorporate varying methods of collecting or analysing data from the quantitative and qualitative research approaches in a single research study [141]. Researchers can collect or analyse numerical data which refers to quantitative research attached with narrative data which is the standard for qualitative research. In this case, the research question(s) are addressed as defined in any typical research study. As an example, mixed methods approach entails that researchers might dispense a survey that contains closed-ended questions to collect quantitative data coupled with conducting an interview by means of open-ended questions to collect the qualitative data [142].

3.2.2 Descriptive Research Design

Descriptive research is meant to provide a picture of a situation as it naturally happens. Due to its pictorial advantage, it could be used to justify a current *modus-operandi* and make judgment. It can also be used to develop theories around a systems activities [141]. A descriptive research design may also be used to explain the state of affairs at present existence [141] . For the purpose of this study, descriptive research was used to obtain pictures of the

current prevailing civil registration systems of birth registration and NRC acquisition in the Republic of Zambia.

3.2.3 Target Group

The study was made up of eight types of target groups of the biometric authentication ecosystem comprising: ICT regulators, Standardization bodies, Consumer protection authorities, students in higher education institutions, banks, Government Ministries and departments, Health Support Institutions and general users. The mentioned respondents were sampled from the: University of Zambia (UNZA), Matem University, Bank of Zambia, Proflight, Stanbic Bank, Zambia Bureau of Standards (ZABS), Zambia Information Communication Technology Authority (ZICTA), Ministry of Home Affairs (Passport Office and Citizen Registration Office), John Snow Initiative (JSi), Ministry of Commerce – National Technology Bureau, Ministry of Information and Broadcasting Services, Competition and Consumer Protection Commission (CCPC), Zambia Development Agency (ZDA) and the study area comprised Lusaka.

The significance of targeting the mentioned groups was meant to capture primary data from the mentioned area through purposive sampling. Purposively sampling signifies how the researcher sees sampling as a series of strategic choices about whom, where and how one does one's research [141].

3.2.4 Sample Size

A total number of 100 respondents were randomly selected for interviews. The researchers hold the view that the sample size was manageable and wide enough for valid generalization to the biometric ecosystem in Zambia.

3.2.5 Data Collection Tools

3.2.5.1 Self-Administered Questionnaires

The self-administered questionnaires were used to collect information from all the respondents. The use of questionnaires was not only simple to administer, but questionnaires were also relatively inexpensive to analyse. As a matter of fact, when alternative replies are

provided in the questionnaires, respondents are able to understand the meaning of questions more clearly.

3.2.6 Data Analysis

Data analysis for the study was done by computer based software known as Microsoft Excel. Microsoft Excel is a paid for computer program that is developed and maintained by the Microsoft Corporation [143].

3.2.7 Ethical Consideration

Ethical clearance was sort from the UNZA ethics committee before undertaking this research. Further permission from the places where the research was conducted from, by means of introductory letters which were given to authorities and respondents. Similarly, all questionnaires administered, did not allow respondents to disclose their names or any information that would review their status and ultimately compromise on confidentiality. Subsequently, all researchers need to be familiar with the basic ethical principles and have up-to-date knowledge about policies and procedures designed in order to ensure that there is safety of research subjects. As such, this prevents sloppy or irresponsible research and any ignorance of policies designed to protect research subjects is not considered a viable excuse for ethically questionable projects.

3.2.8 Limitation of the Baseline Study

The ideal situation was to collect data from all the ten provinces of Zambia. However, it was difficult to achieve the intended purpose due to financial and time constraints. The prototype is designed to enhance the civil registration processes in the republic of Zambia and as such live tests can only be performed at the Ministry of Home Affairs and partly with the Ministry of Health (MoH). Getting permission for a live test with these institutions implies collecting citizen data. This was inhibitive. The other limitation was from some target groups like: commercial banks and some government offices that deal with citizen data who entirely refused to take part in the survey for fear of disclosing their information to the general public.

3.2.9 Presentation of Findings

Presentation of findings was done through summarized presentations in form of various tables and figures in order to facilitate understanding.

3.3 System Design Methodology

It is important to realize that the system requirements specification and model design phase of the research study employed, hinges on the use of qualitative data gathered from reading through the GRZ General Affidavit Form N, Hospital Birth Record, Under-five children's clinic card, GRZ Birth Certificate, through interviews of respondents at the Ministry of home Affairs and observation of the civil registration process at the Ministry of Home Affairs. The other respondents which included: general users and regulators were interviewed in order to gather information concerning the biometric ecosystem in Zambia. As such, all the respondents provided the qualitative data that is needed to specify requirements for the system, design models coupled with developing the system prototype for civil registrations.

The methodology used for the analysis, design and development of the software system is the object-oriented systems development methodology (OOSDM). This research study utilized some of the diagrammatic representations that are present in the unified / universal modeling language (UML) in order to visualize the system from various perspectives [144] [145].

The object-oriented system development (OOSD) approach that was used in the system development process is one that is use case driven. The object-oriented system development life cycle (OOSDLC) was used for the system development in this research study in order to show multiple iterations to be carried out throughout the entire development cycle for the system to be gradually built in small modular increments [146].

A mind-map illustrating the study is placed in the appendix for further comprehension.

3.3.1 Current Business Process in the Civil Registration System

Figure 3.1 shows the current civil registration processes for both urban and rural environments as performed in Zambia.

With reference to Figure 3.1, it is mandatory for all Zambian citizens to be registered with the Ministry of Home Affairs. To achieve this feat, GRZ ensures that in urban birth situations birth records are used as source records of birth data. As shown in figure 3.1 the urban civil

registration business process is highlighted with black process flows while the rural are highlighted with red process flows.

In Figure 3.1 for urban processes; a birth occurring at an urban health facility will have a birth record issued (Figure 3.2a and Figure 3.2b). This document becomes a source record that can will be used in conjunction with a sworn affidavit form (Figure 3.4) when applying for a birth certificate. Processes 1 – 6 illustrate these processes. A successful application yields a birth certificate (Process 7).

In Figure 3.1 for rural processes; a birth occurring at a rural centre will be registered with the village authority. The village authority document becomes a source record when and is used in the award of an under-five clinic card at any nearest health facility. The village authority document, under-five clinic card and affidavit form are source documents when applying for a birth certificate. Processes 1 – 9 illustrate these processes. A successful application yields a birth certificate (Process 10).

Figures 3.2a and 3.2b show samples of a birth record.

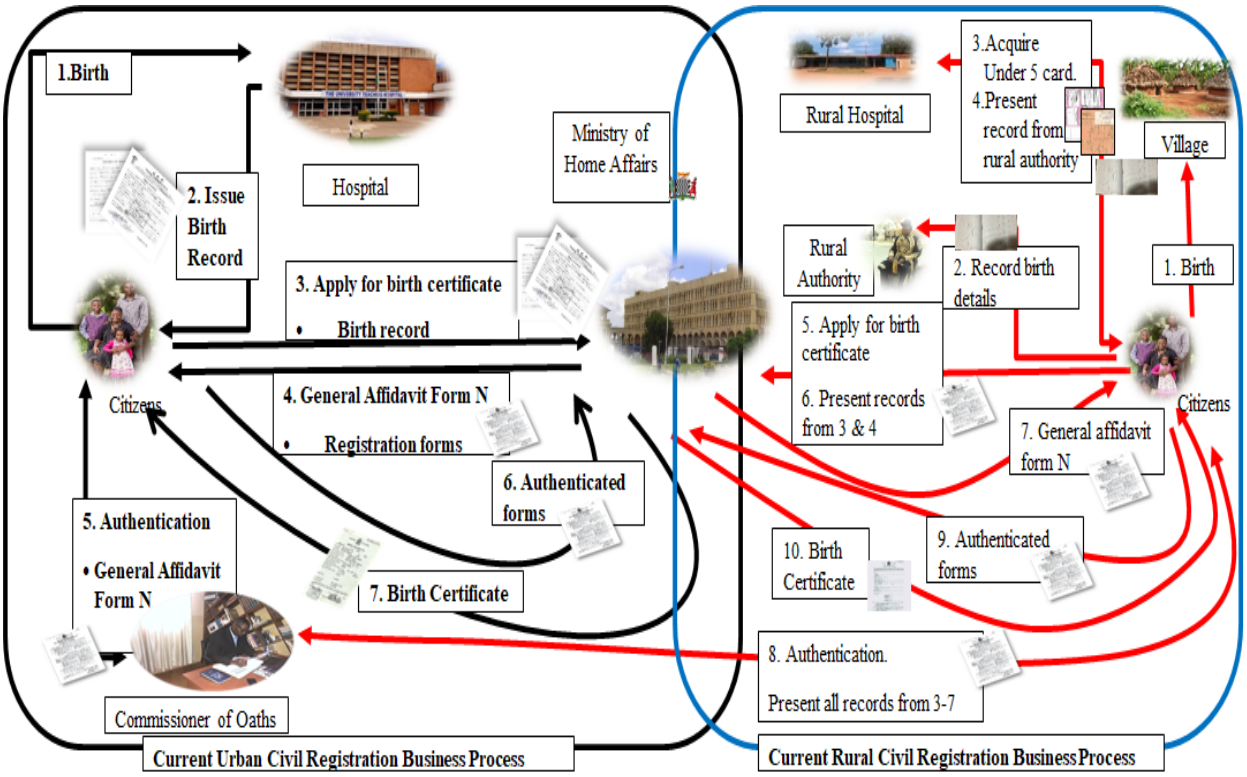


Figure 3.1. Current Business Process – Urban and Rural Process

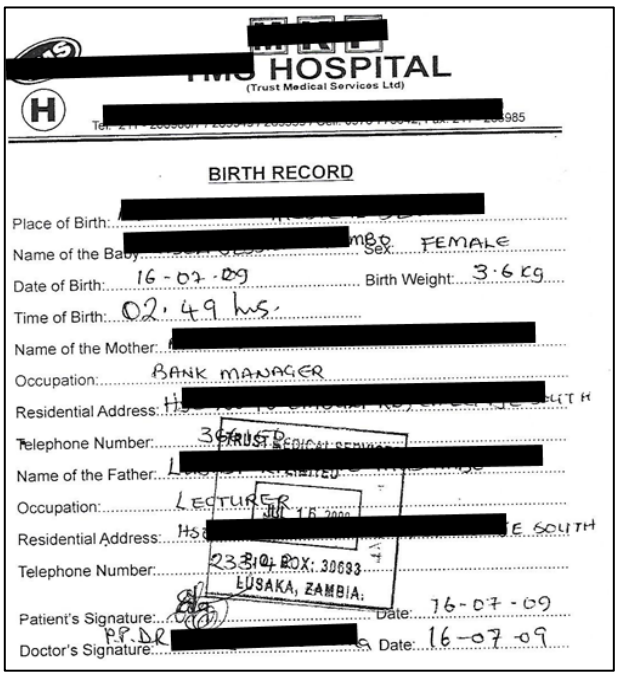


Figure 3.2a. Sample of a Birth Record

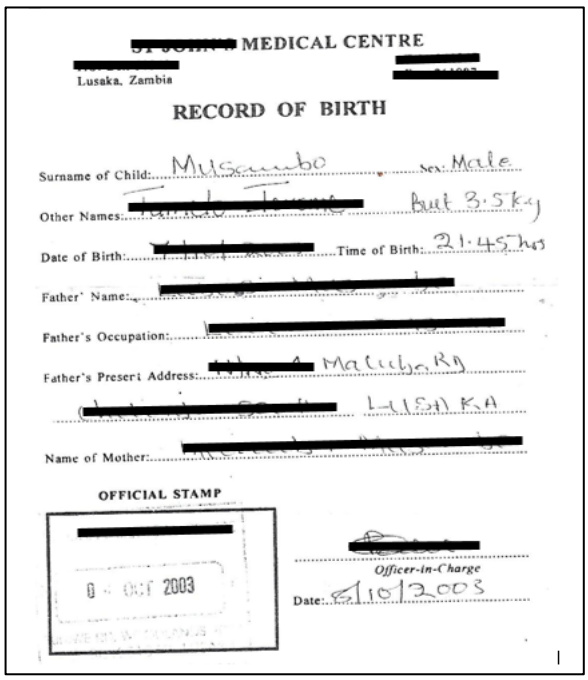


Figure 3.2b. Sample of a Birth Record

In rural, Zambia, birth is recorded via the village authority in what is referred to as a village register. This is because most of the births occur outside a health facility. Sialubanje et al. assigns several reasons for this occurrence, among them being [147]:

i. Women's lack of decision-making autonomy regarding child birth;
ii. Dependence on the husband and other family members for the final decision;
iii. Physical and socioeconomic barriers such as long distances to health facilities;
iv. Lack of money for transport to the health facilities;
v. The requirement to bring baby clothes and food while staying at the health facility which appears to be cost driven;
vi. Socio-cultural norms regarding childbirth such as the health facility staff may not be skilled, maybe rude, cannot be trusted and lack respect;
vii. Negative attitude towards the quality of services provided at the clinic.

The village birth is then recorded at any nearest health facility using the village register record as authentication of birth. At the nearest rural health facility, the birth details are recorded onto an under-five clinic card. Figure 3.3a and 3.3b show samples of the under-five clinic card. Both the village record and under-five clinic card work as source records of birth.

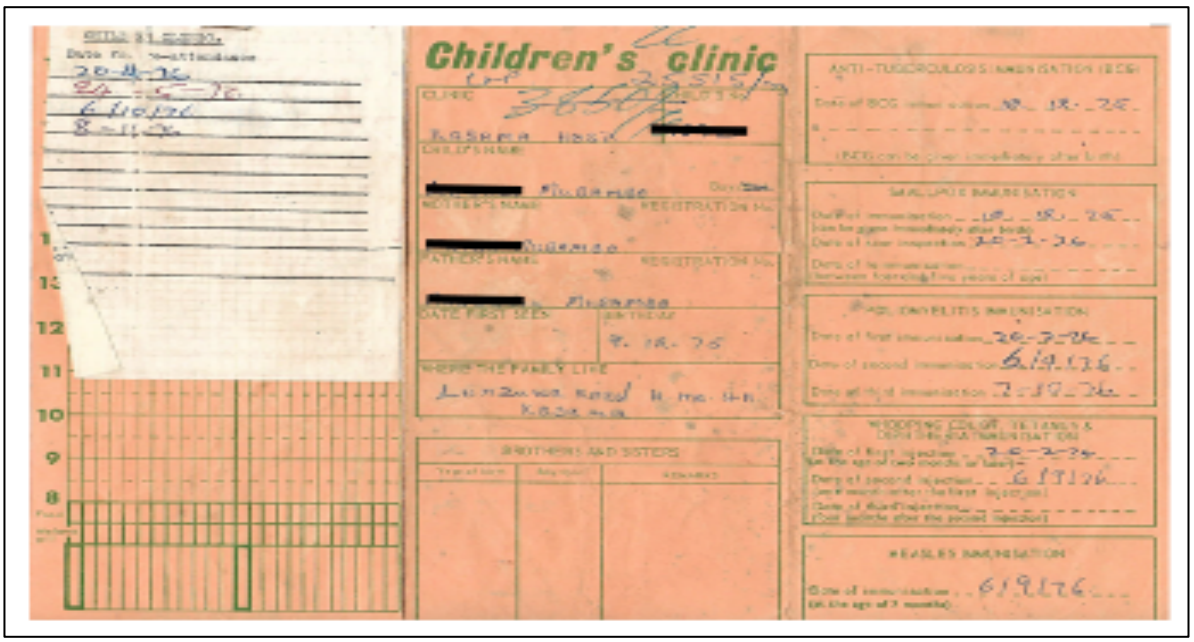


Figure 3.3a. Sample of an Under-five Clinic Card

The information from the source records are then used as input to a registration form and General Form Affidavit N when applying for a birth certificate. The General Form Affidavit Form N which is sworn by any individual recognised by GRZ as a commissioner of oath works as an authentication tool of the birth to GRZ. Should all records be acceptable and meet the minimum requirements for a birth certificate, GRZ will issue a birth certificate.

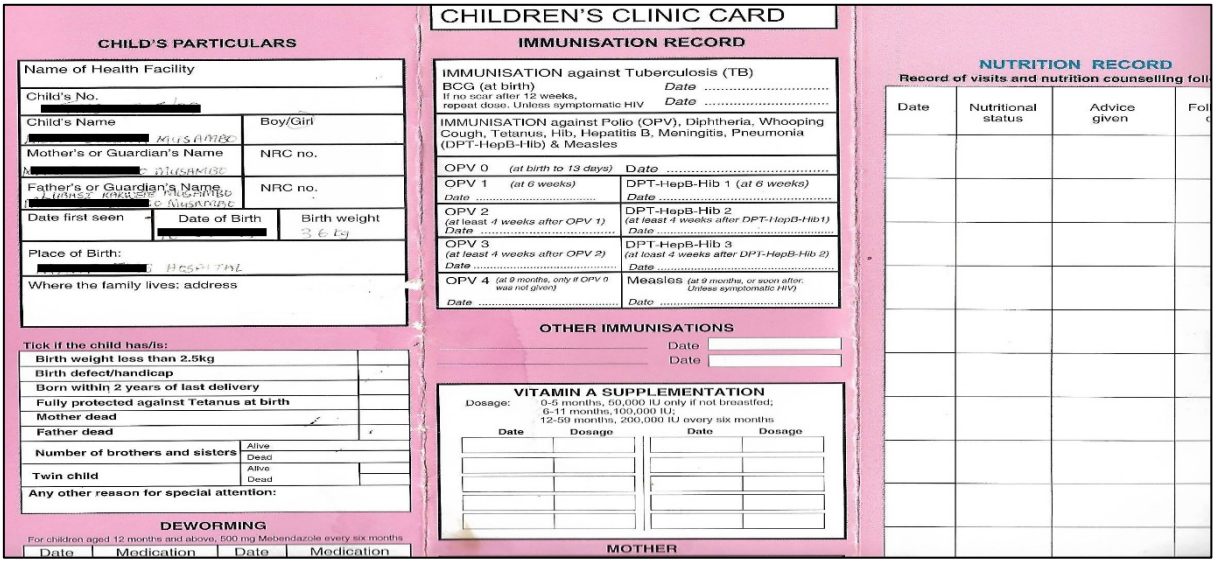
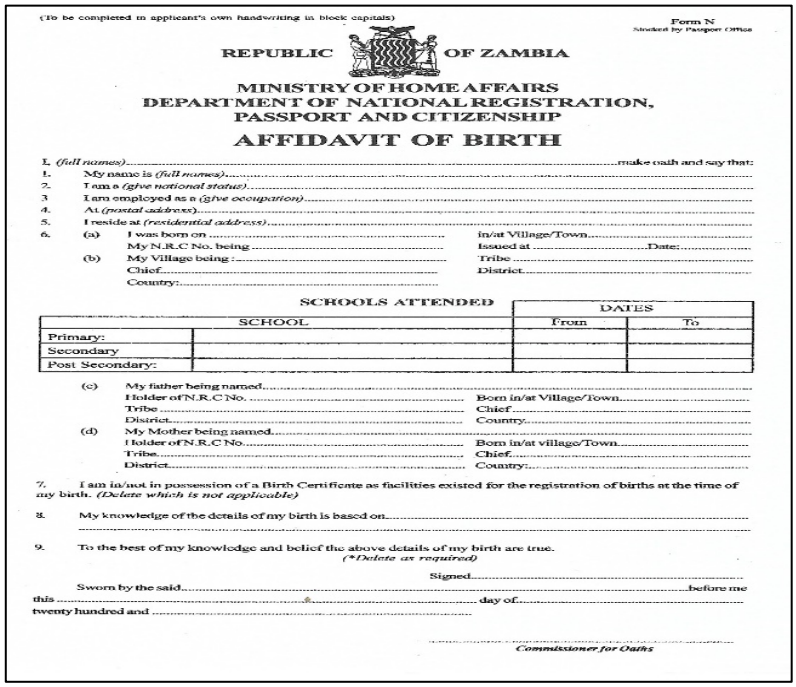


Figure 3.3b. Sample of an Under-five Clinic Card

Should a Zambian citizen attain sixteen years of age, he/she is entitled to a NRC. The NRC requires a submission of a birth certificate, sworn General Affidavit Form N and an application to GRZ before it can be issued to the deserving individual. Figure 3.4 shows a sample of a General Affidavit Form N, Figure 3.5 shows a sample of a NRC and Figure 3.6 shows a sample of a birth certificate.



(To be completed in applicant's own handwriting in block capitals) Form N Stocked by Passport Office

REPUBLIC OF ZAMBIA

MINISTRY OF HOME AFFAIRS
DEPARTMENT OF NATIONAL REGISTRATION, PASSPORT AND CITIZENSHIP

AFFIDAVIT OF BIRTH

I, *(full names)* ..... make oath and say that:

1. My name is *(full names)* .....
2. I am a *(give national status)* .....
3. I am employed as a *(give occupation)* .....
4. At *(postal address)* .....
5. I reside at *(residential address)* .....
6. (a) I was born on ..... in/at Village/Town .....
   My N.R.C No. being ..... Issued at ..... Date: .....
   (b) My Village being: ..... Tribe .....
   Chief ..... District .....
   Country: .....

SCHOOLS ATTENDED		DATES	
SCHOOL		From	To
Primary:			
Secondary			
Post Secondary:			

   (c) My father being named ..... Holder of N.R.C No. ..... Born in/at Village/Town ..... Tribe ..... Chief ..... District ..... Country .....
   (d) My Mother being named ..... Holder of N.R.C No. ..... Born in/at village/Town ..... Tribe ..... Chief ..... District ..... Country: .....
7. I am in/not in possession of a Birth Certificate as facilities existed for the registration of births at the time of my birth. *(Delete which is not applicable)*
8. My knowledge of the details of my birth is based on .....
9. To the best of my knowledge and belief the above details of my birth are true. *(*Delete as required)*

Signed .....

Sworn by the said ..... before me this ..... day of ..... twenty hundred and .....

Commissioner for Oaths

Figure 3.4. Sample of a General Form Affidavit N

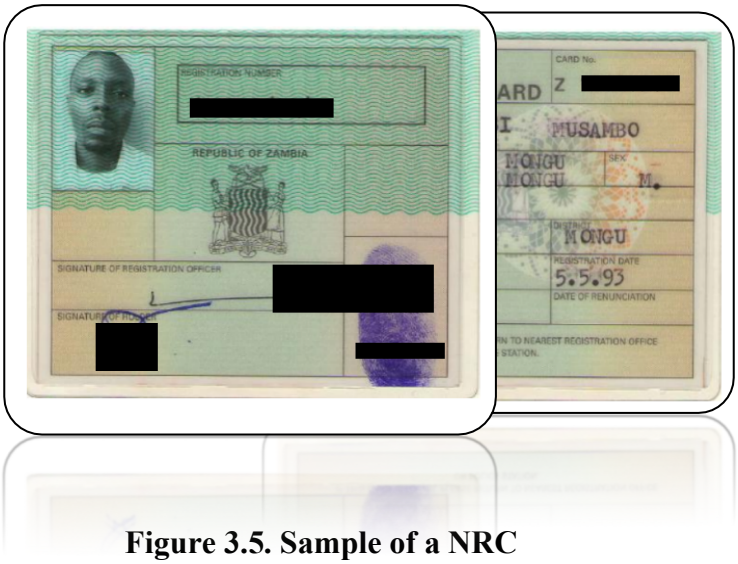
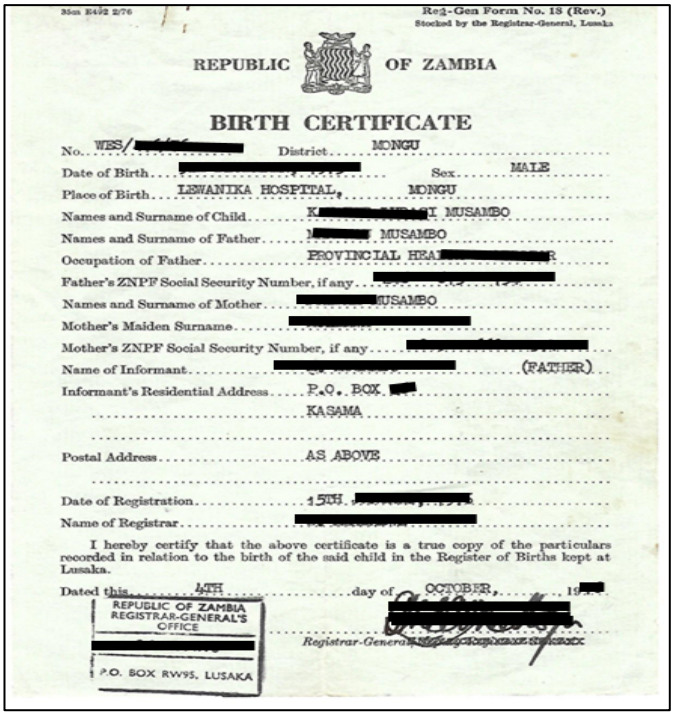


Figure 3.5. Sample of a NRC



Reg.-Gen Form No. 18 (Rev.)
Stocked by the Registrar-General, Lusaka

REPUBLIC OF ZAMBIA

BIRTH CERTIFICATE

No. WES/[redacted] District MONGU
Date of Birth [redacted] Sex MALE
Place of Birth LEWANIKA HOSPITAL, MONGU
Names and Surname of Child [redacted] MUSAMBO
Names and Surname of Father [redacted] MUSAMBO
Occupation of Father PROVINCIAL HEA[redacted]
Father's ZNPF Social Security Number, if any [redacted]
Names and Surname of Mother [redacted]USAMBO
Mother's Maiden Surname [redacted]
Mother's ZNPF Social Security Number, if any [redacted]
Name of Informant [redacted] (FATHER)
Informant's Residential Address P.O. BOX [redacted]
KASAMA
Postal Address AS ABOVE
Date of Registration 15TH [redacted]
Name of Registrar [redacted]

I hereby certify that the above certificate is a true copy of the particulars recorded in relation to the birth of the said child in the Register of Births kept at Lusaka.

Dated this 4TH day of OCTOBER, 19[redacted]

REPUBLIC OF ZAMBIA
REGISTRAR-GENERAL'S OFFICE
[redacted]
P.O. BOX RW95, LUSAKA

Registrar-General

Figure 3.6. Sample of a Birth Certificate

Due to the lack of standard to be applied in the birth record format as shown in Figures 3.2a and 3.2b, it is possible to ignore certain information during data collection as some certificates may not have certain fields while other birth records from other hospitals may contain extra fields. This type of information collection creates a problem of a lack of consistency.

Due to the fact that General Affiidavit Form N is used to authenticate the birth details before the details are captured by the GRZ through MoHA, a possibility of corrupting a comissioner of oath by a non-Zambian individual so that he/she provides a sworn affidavit exists.

Due to collection and recollection, capturing and recapturing of the same information concerning the same individual during the registartion process a problem of information redundancy is created.

Due to the storage of information at isolated different points about the same individual as seen from the business processes, a possibility of data theft is created, a possibility of loss of information integrity is created.

A change of information at one point within the business process will require existensive effort to correct this information at all centers, this is a problem of islands of information. This also creates a problem of repeated effort.

3.3.2 Proposed Civil Registration System

The optional civil system for this study involves a civil registration model termed, *'VitalReg'* which is designed to be used on the internet. The new system's objective is to give an improved method to the collection of vital statistics in a secured way by employing biometrics, encryption and 2FA by attempting to automate the entire process by keeping the view of database integration approach through the following activities:

a) Provision of user friendliness in the application's processes through the available controls that are provided by the system's user interface;
b) Ability to create users; both administrators and non-administrator users on the system in an easy manner;
c) Ability to capture facial face dataset that are used in the biometric authentication of individuals;
d) The ability to perform a face recognition and identification with a 66% acceptance rate;
e) The integration of spatial data within the model that allows the program to generate a GPS location of the registration centre and integrate this data into the output for audit purposes;
f) The ability to encrypt the stored data within the database which works as a contraceptive to data theft as the data cannot be understood once accessed;
g) The application generates a QR Code on output. This QR Code contains details about the registered individual. Details such as the registration date, sex of the individual and certificate number are embedded in the QR Code. The QR Code can work as a second authentication factor in addition to the biometric facial feature authentication.

   Figures 3.7 and 3.8 show the code snippets for the geospatial data and QR Codes respectively.
h) The model allows for an easy database interrogation of its details through a down-down combo-box option.

```
. . .    jQuery("#btnInit").click(initiate_geolocation);
    })
    function initiate_geolocation() {
        if (navigator.geolocation)
        {
navigator.geolocation.getCurrentPosition(handle_geolocation_query,
handle_errors);
        }
        else
        {
            yqlgeo.get('visitor', normalize_yql_response);
        }
    }
    initiate_geolocation();
     function handle_errors(error)
    {
        switch(error.code)
        {
            case error.PERMISSION_DENIED: alert("user did not share
geolocation data");
            break;
            case error.POSITION_UNAVAILABLE: alert("could not detect
current position");
            break;
            case error.TIMEOUT: alert("retrieving position
timedout");
            break;
            default: alert("unknown error");
            break;
       }
    }
     function normalize_yql_response(response)
    {
        if (response.error)
        {
            var error = { code : 0 };
            handle_error(error);
            return;
        }
        var position = {
            coords :
            {
                latitude: response.place.centroid.latitude,
                longitude: response.place.centroid.longitude
            },
            address :

            {   city: response.place.locality2.content,

                region: response.place.admin1.content,

                country: response.place.country.content
            }  . . .
```

Figure 3.7. Code snippet: Geospatial

```
. . .
var qrcode = new QRCode("qrcode", {
    width: 120,
    height: 120,
  });
function makeCode () {
  var elText = document.getElementById("qrcodes_map");
  if (!elText.value) {
    alert("Input a text");
    elText.focus();
    return;
  }
  qrcode.makeCode(elText.value);
}
makeCode(); . . .
```

Figure 3.8. Code Snippet: QR Code Mapper

Advantages that the proposed civil registration model brings can be seen as aiming at addressing the drawbacks that the current civil registration system has. Some of the advantages of this civil registration system are:

a) Enabling citizen registration;
b) Enabling users to obtain their vital event documents on the spot without the need to wait for up to 3 months as in the current processes;
c) Speeds up the work for GRZ and in particular MoHA as far as civil registration is concerned. This has the effect of improving the GRZ service delivery;
d) Secured central data storage that guarantees the civil records have integrity;
e) Web-based system that can allow for a use at any centre within Zambia;
f) Spatial data integration that allows for quick audit of where civil records are generated;
g) Citizen authentication and repudiation factors are accounted for.

3.3.2.1 Overall business processes flow for the proposed model

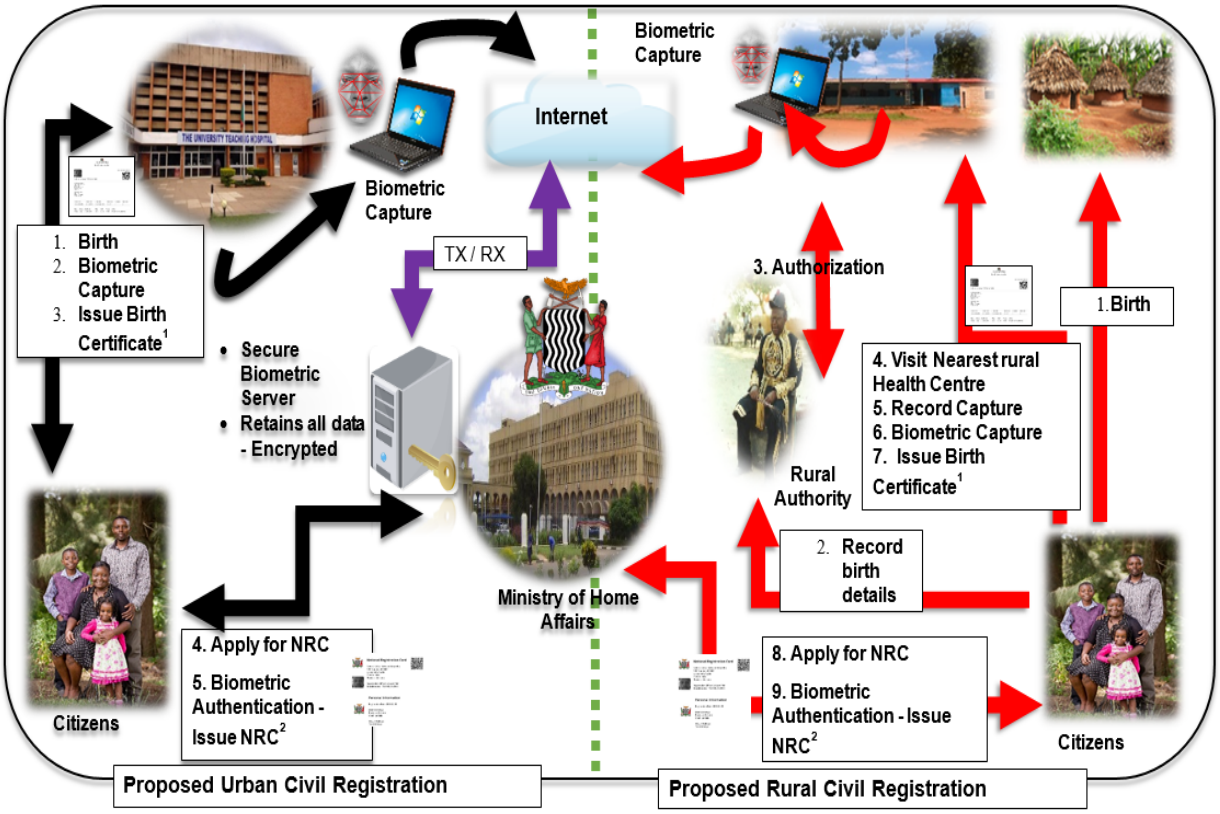


Figure 3.9. Proposed Civil Registration Business Processes

This section, illustrates the transactions that will be carried out in the proposed civil registration system. Figure 3.9 describes the steps that would be involved from source (i.e. start) to end (i.e. stop) of the civil registration process until a vital event document is issued. The processes are numbered for easy follow through.

3.3.2.2 Urban Civil Registration

A birth occurring at an urban health facility will be registered there and then. The facial features will be captured and all other vital event circumstances will be captured at source (birth place). A birth certificate will be issued at source. The birth vital data shall be sent electronically to the MoHA via networks into a secured biometric server. Urban birth occurring outside a health facility shall be recorded as above at any nearest health facility to the birth occurrence. The biometric data on the server shall be encrypted at source and sent in encrypted state through networks up to the server. The encryption shall ensure the information is hidden in plain sight. For purposes of prototype demonstration, the current encryption has

been set to base 64 encryption which is a binary-to-text encoding scheme that represent binary data in an ASCII (American Standard Code for Information Interchange) string format by translating it into radix-64 representation [148].

Base 64 is a 64bit encryption algorithm with a reasonable cover time. In cryptography, cover time is a theoretical security of a cipher that depends on the available computer processing and the key length [46]. For purposes of explanation we can assume that an individual who has intentions of stealing the civil database that is generated from the proposed civil registration prototype had a computing resource of 2 GHz processing capability then such an attacker would have to contend with the 64 bit encryption for approximately 159years.

For purposes of demonstration of the strength of the 64bit encryption used, the concept of time is calculated as follows:

Let Cover Time = C_t; C_p = Computational Complexity; C_s = Computer Speed (processor Speed)

Therefore:

$$C_t = \frac{C_p}{C_s} \qquad (4)$$

$$\frac{C_p}{C_s} = \frac{2^{64}}{2x10^9} \approx \mathbf{159}\boldsymbol{years}$$

The author hold the view that at a computational speed of 2GHz, the cipher holds for an approximate 159 years and this gives sufficient guarantee for the privacy of the civil data maintained in the database.

Part of the code snippet responsible for the encryption is shown in Figure 3.11:

```
$gencode =
base64_encode($person_id.'/'.$father_nrc.'/'.$generate3.'/'.$
register_date);
```

Figure 3.10. Code Snippet: Encryption Encoder

When the database is viewed it will display data that cannot be understood as the information displayed is in a form that cannot make intelligible sense. A sample of the database representation is shown in Figure 3.11:

id	f_name	m_name	s_name	sex	nrc_num	dob	address	birth_hospital	district	town	chief	mother_nrc	mother_ssn	father_nrc	father_ssn
8	Emmanuel	Tinashe	Lungu	Male	000001	MTk3NS8xMi8wOQ=	18 Kakuzi Road	nknkj	Luangwa	Luangwa	Mburuma	MDk5MA==	MTExMTExLzExLzE=	MzMzMzMzLzExLzE=	MjIyMjIyLzExLzE=
10	Lubasi	Kakwete	Musambo	Male	000002	MTk3NS8xMi8wOQ=	801/33a Vorna Valley, Meanwood	Lewanika General	Mongu	Mongu	Kandala	NA==	MQ==	Mw==	Mg==
12	Ken	NA	Mulenga	Male	000004	MTk3NS8wOC8xNA=	2 Kudu Road	Masala Clinic	Luwingu	Lusaka	Chungu	NDQ0MzM2LzY1LzE=	NjY1NTU0MzMyMjIx	MzMzMzM0LzY2LzE=	Nzc2NTU0NDQzMzMy

Figure 3.11. Sample Civil Database Output

As can be seen in Figure 3.11, the information to do with date of birth *(dob)*, mother's NRC *(mother_nrc)*, mother's social security number *(mother_ssn)*, father's NRC *(father_nrc)* and father's social security number *(father_ssn)* are all non-intelligible. This is the result of the encryption. Figure 3.12 shows the code snippet for the face detection and face capture that used by the model to detect a face and capture a face from which Haar-like features can be extracted to form a strong classifier.

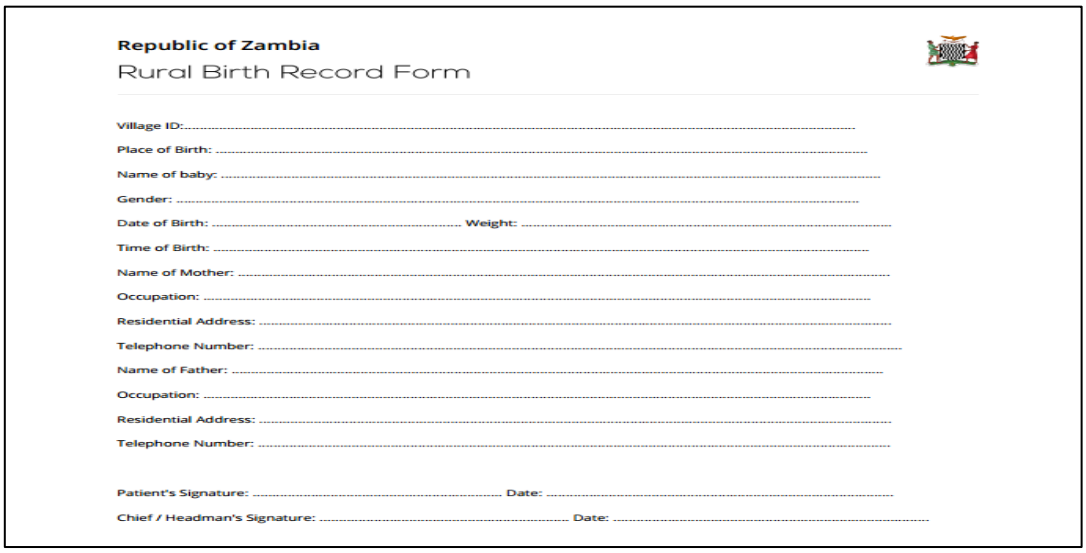
```
.   .   .   faces = faceCascade.detectMultiScale(gray, 1.2,5)
    # Get face from video frame then using for create integral, begin  . . .
    for(x,y,w,h) in faces:
        # Create integral, begin.  .  .
        cv2.rectangle(im, (x-20,y-20), (x+w+20,y+h+20), (0,255,0), 4)
        # attach face to ID, begin  .   .   .
        Id, confidence = recognizer.predict(gray[y:y+h,x:x+w])
        new = 1
        url = 'http://localhost/vital/vital_docs?id={}'.format(Id)
        webbrowser.open(url, new=new)
        cam.release()
        cv2.destroyAllWindows()
        # label person in pic, begin .   .   .
        cv2.rectangle(im, (x-22,y-90), (x+w+22, y-22), (0,255,0), -1)
        cv2.putText(im, str(Id), (x,y-40), font, 1, (255,255,255), 3)
    # Display video frame with bound rectangle, begin.  .  .
    cv2.imshow('Vital Recognition',im)
    # If 'q' is pressed, quit face recognizer, begin .  .  .
    if cv2.waitKey(10) & 0xFF == ord('q'):
        break
# Shut camera, invoke win control module, begin .   .    .
```

Figure 3.12. Code Snippet: Face Detection, Capture. Adapted from [138] [139]

The database has been developed using MySQL. The prototype has been developed using php, HTML, JavaScript, python, CSS, batch files and uses the XAMPP control panel to manage the server abilities on standalone computing resources. These technologies have been chosen due to their open-source nature which introduces cost-effectiveness [149]

3.3.2.3 Rural Civil Registration

A birth occurring in rural centers will be registered with the village authority initially then with the nearest health facility. The village authority shall be trained to access a template of birth from the civil registration program that can be used to collect birth details. This birth template makes the birth record standard and uniform throughout rural Zambia. The template is then presented to the health facility where a biometric capture is made of the child and birth details collected into digital form. Figure 3.13 shows the birth template. Operations after the biometric capture are equivalent as in the urban birth registration.


Republic of Zambia

Rural Birth Record Form

Village ID:.....

Place of Birth: .....

Name of baby: .....

Gender: .....

Date of Birth: ..... Weight: .....

Time of Birth: .....

Name of Mother: .....

Occupation: .....

Residential Address: .....

Telephone Number: .....

Name of Father: .....

Occupation: .....

Residential Address: .....

Telephone Number: .....

Patient's Signature: ..... Date: .....

Chief / Headman's Signature: ..... Date: .....

Figure 3.13. Sample Birth Template

3.3.2.4 Areas of use

The use of the prototype can be categorized into the following 5 groups: Civil Database, Biometric Authentication for Electronic Voting, Student Facial Authentication, Crime Management and Death Management.

i. Civil Database: a possibility exists that allows the prototype to be used as a storage for all citizen civil registration. That way no island of information would exist;
ii. Biometric Authentication for Electronic Voting: a possibility exists that can allow the prototype be used to perform authentication of individuals before a vote is made in the

Republic of Zambia's elections. Because the prototype would house all civil data, there would be no need to register anyone for an election, in this manner the strenuous process of voter registration would not exist. Individuals desiring to participate in the vote process would simply present themselves to a polling station where a biometric authentication would be made, and a vote allowed;

iii. Student Facial Authentication: Higher institution of learning would make use of the prototype to perform an authentication on students within a learning institution so that the students are awarded school services should they pass the authentication;

iv. Crime Management: The law enforcement agencies can use the facial authentication facility to carry out identification and recognition of individuals or suspects during an investigation;

v. Death Management: the facial recognition and identification can be used to carry out identification of individuals who have died but do not have identification documentation on them. Further, once a positive identification is made, the prototype can be further modified to allow for a change in the records of that individual to indicate 'deceased'.

3.4 System Architecture

3.4.1 Civil Registration system Architecture

The following explanation is based on Figure 3.14.

Figure 3.14 shows how a system user found at a civil registration point would interact with the system. The citizen would present themselves then a biometric capture is done using a web camera. The civil registration system uses a web camera to capture the face image of a subject.

The prototype captures a maximum of 100 faces. Once captured the system user would run a calibrator to pick the facial features. The facial features are picked by the Haar Cascade Algorithm. Once this is done a calibration must be done. This implies the process of picking what are termed as weak classifiers and combining them into a strong classifier so that a facial recognition can be done. Once this is complete, a trail biometric run must be made to confirm that the subject has been correctly enrolled. In the case of a false rejection rate [107] which is at 33% % a re-enrolment must be done.

The details are transmitted via a firewalled network as shown in processes labelled 2.

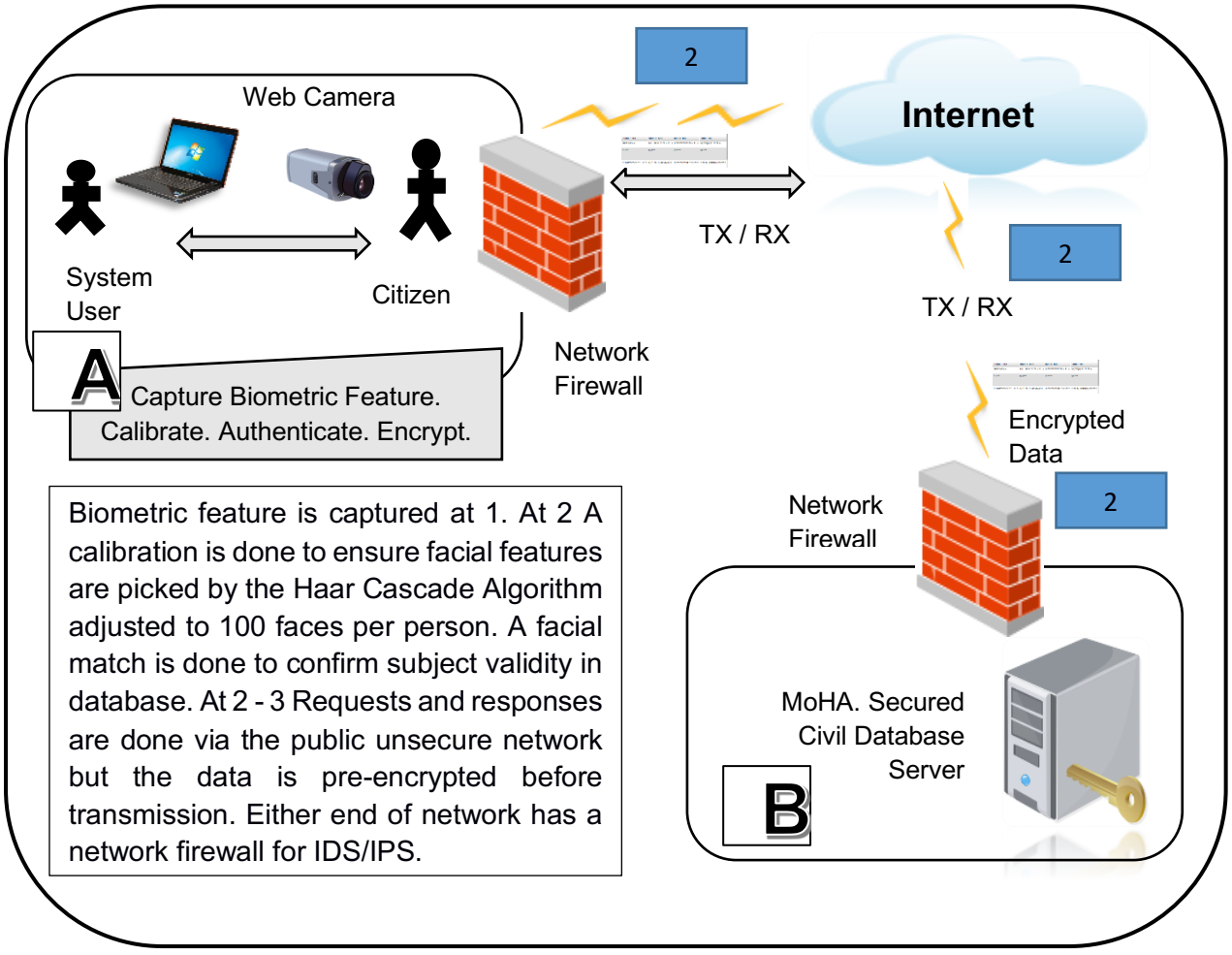


Figure 3.14. System Architecture for the civil Registration System

The use of a public network is advantages as it reduces the cost of the system operation. The data is transmitted over the internet in an encrypted form as shown in processes '2'. The firewalled network works as a contraceptive to network intrusion threats and data theft over networks [53]. The database is setup at the MoHA and is developed into a secured server with security logins needed to access the server services. The processes at **A** form the user-end and at this end, no data processing is done. All processing is performed at the central server at process '**B**'. **B** is the server-end of the system which shall process all work and provide feedback to the user-end. No data shall be kept at process **A** to eliminate islands of information [150]. Tx / Rx in this case is taken to imply the transmission of data over a network. The computer unit with key and apparent lock mechanism depicts a secured server.

Figure 3.15 shows the interaction sequence for the proposed system.

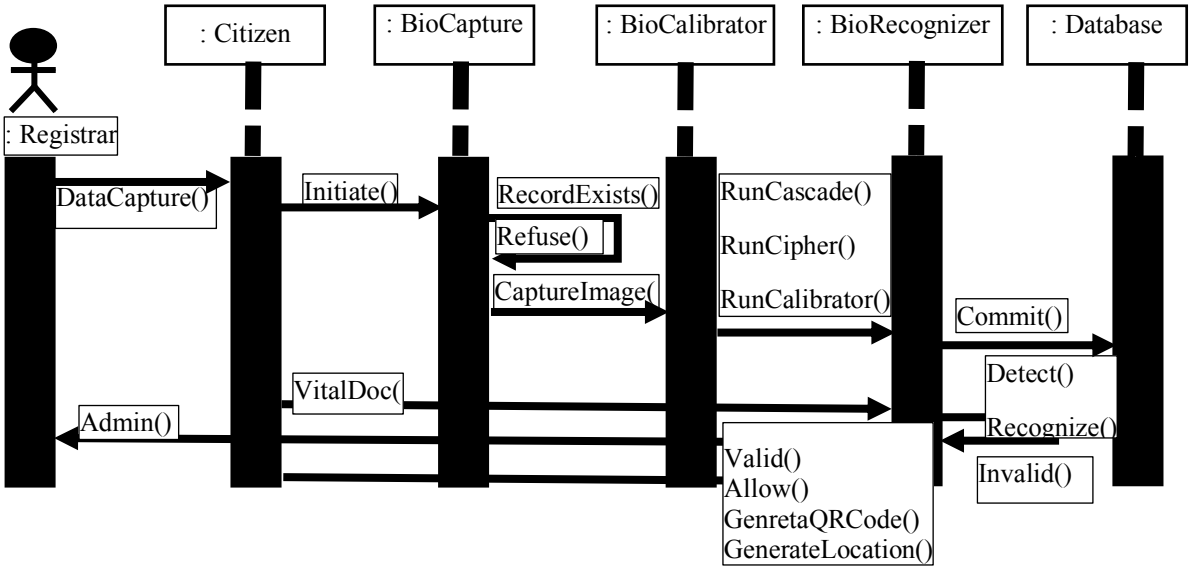


Figure 3.15. Interaction Sequence for Proposed Model.

3.4.2 The operation of the Haar Cascade Algorithm

Based on a rapid object detection scheme based on boosted cascade of simple feature classifiers introduced by Paul Viola and Michael Jones [138], a facial biometric model can be developed based on Haar-like features and implemented to detect and recognise a citizen's face [106] [139] [107]. This recognition facility allows for authentication. Facial features to form a Haar classifier are collected after a facial mapping as shown in Figure 3.15. The biometric model utilises Haar basis features as used by Papageorgiou et al [151].

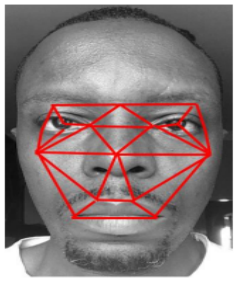


Figure 3.16. Identifying features by a biometric reader. Adapted from [137]

An adaption of the algorithm based on an OpenCV Open Source technology which is readily available from OpenCV has been used [152]. This algorithm uses Haar like features and OpenCV pre-trained classifiers for face detection. A classifier is a program that can decide whether an image is positive or not. A positive image is an image face (image having a face) while a negative image is a non-face image [152]. Classifiers are

trained from a huge volume of faces (both positive and negative images) to learn how to classify a new image correctly. This is a machine learning concept. The classifiers used for this student authentication is the HaarClassifier which is earlier developed by Viola et al [138]. Haar Classifiers process data in grey scale (non-colour). Colour is inconsequential in determining whether an image has a face or not [106]. Viola et al states each object has features that are unique and can be used to identify and recognize that object. Haar features can be picked out from edge, line, centre and diagonal features of an object as shown in Figure 3.17.

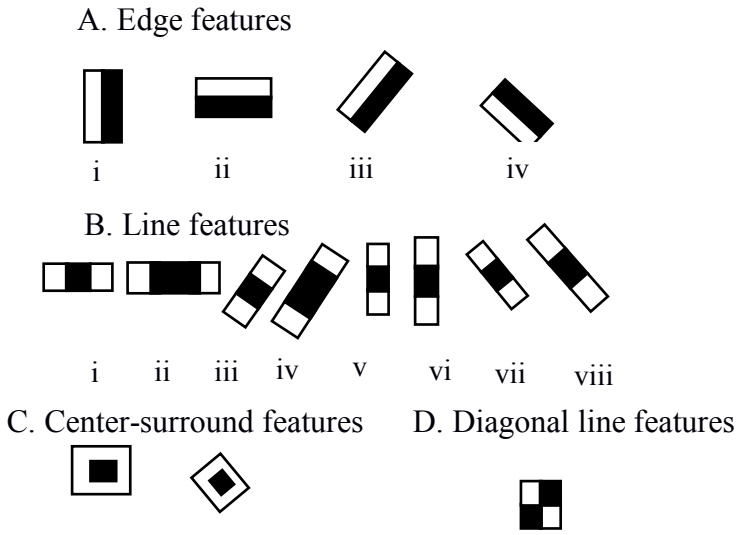


Figure 3.17. Feature determination. Adapted from [139] [153] [107] [165]

Edge features are characteristics of an image that are unique and at unique distances from each other [139] [53]. No two people share the same features. These features can be mapped by placing an object identifying feature on an image [153]. A biometric model developed to pick up the readings from the facial recognizer can pick up the features and collectively store them to perform identification and recognition. The features can be

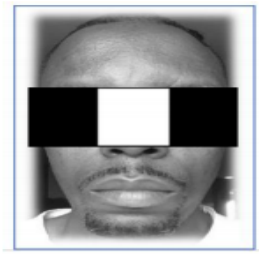


Figure 3.18. Feature Extraction. Adapted from [106] [104]

collected into small elements referred to as a weak classifier which when collectively used identify and recognize an object [107]. Feature collection is done via rectangles. Haar like features consist of two or more rectangular regions enclosed in a template. Each of the rectangles is a window that is placed on an image as shown in Figure 3.18 that is to be captured and recognized. A feature is extracted from subtracting the sum of pixels under the white part from the black part of that window (rectangle).

In determining the haar like features an understanding that the area around the eyes have a darker area then the nose bridge is used. This view is also held for the cheeks (brighter than other areas), though the data from the cheeks is not necessarily used [152]. Rectangles are placed on an image so as to pick the features using a weak classifier [139]. The features of a rectangle are computed using an integral function of the form:

$$ii(x, y) = \sum_{x' \leq x, y' \leq y} i(x', y'), \quad (5)$$

In this function an object or image at location x, y contains the sum of pixels above and to the left of x, y inclusive.

Where, ii (x, y) and i (x, y) is the original image. Using the following pair of recurrences:

$s\,(x, y) = s(x, y - i) + i\,(x, y)$

$ii\,(x, y) = ii(x\text{-}i, y) + s(x, y)$

(Where s(x, y) is the cumulative row sum, $s\,(x\text{-}a) = 0$, and $ii\,(-i, y) = 0)$. Using the integral image any rectangular sum can be computed in four array references. The rectangle itself can be understood to have an object of pixels $W x H$ (i.e.to say width x Height) [106]. Figure 3.19 shows the determination of a rectangular region of an integral image.

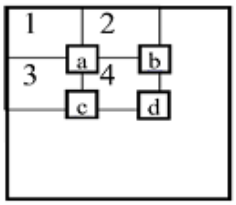


Figure 3.19. Rectangular regions of an integral image [165]

To determine the sum of pixels, the logic can be deduced as follows:

$a = sumRec\ (pixels)$ (6)

$b = 1 + 2,$

$c = 1 + 3$

$d = 1 + 2 + 3 + 4$

The sum is then derived as $d + a - (b + c)$.

3.4.5 User interface specification

3.4.5.1 Introduction

The user interface specification is a complete description of the API (Applications Programming Interface) and what the interface looks like to the user from the designers' point of view.

3.4.5.2 User interface description

The interface for the user is developed in a simple easy to manoeuvre entity that incorporates a simple, visually relevant or significant front in order to ensure that usability design principles are met. The user interface is developed in such a way that it not crowded with unnecessary information and is deliberately designed to guide a user during a systems operation with clearly labelled objects and user friendly prompts when needed. A system user will be met by a consistent screen interface when carrying out operations. Invoking the program is done through clicking the icon displayed in Figure 3.20.

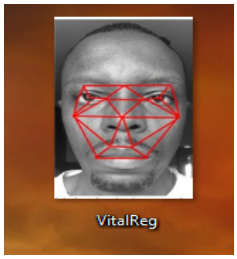


Figure 3.20. Civil Registration System Icon

3.4.5.3 How the user interface looks and behaves

When the program is invoked, a login screen greets a user. Figure 3.21 shows the login screen. To proceed further, user credentials are needed. This screen forms the first-level security of the model.

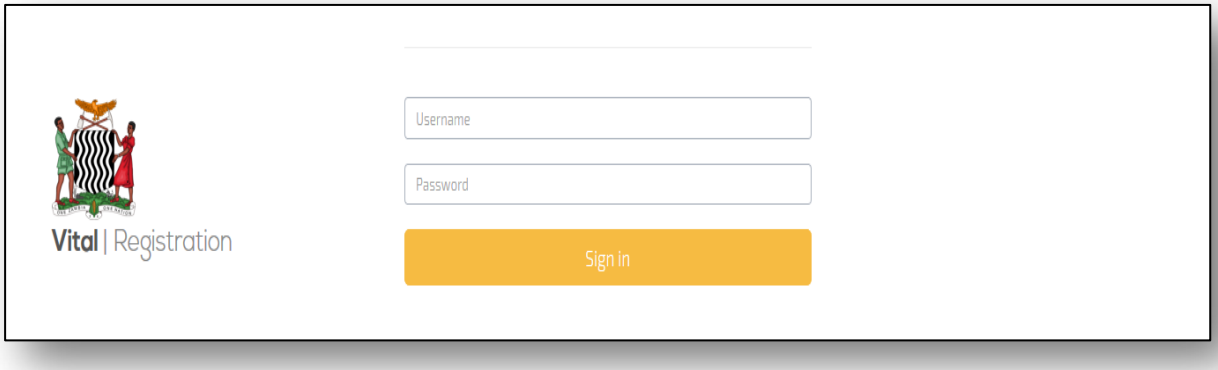


Figure 3.21. Login Screen

In the case of a first time run, default login credentials have been set to:

Username: admin

Password: 123456

Entering these credentials allows one access to the administrator operations of the program where a sub user can be created. The difference between the system administrator login and sub-user login is that the systems administrator can allow user creation while the sub user cannot allow this feature. Login password is masked for security purposes. Figure 3.22 illustrates the masked password input.

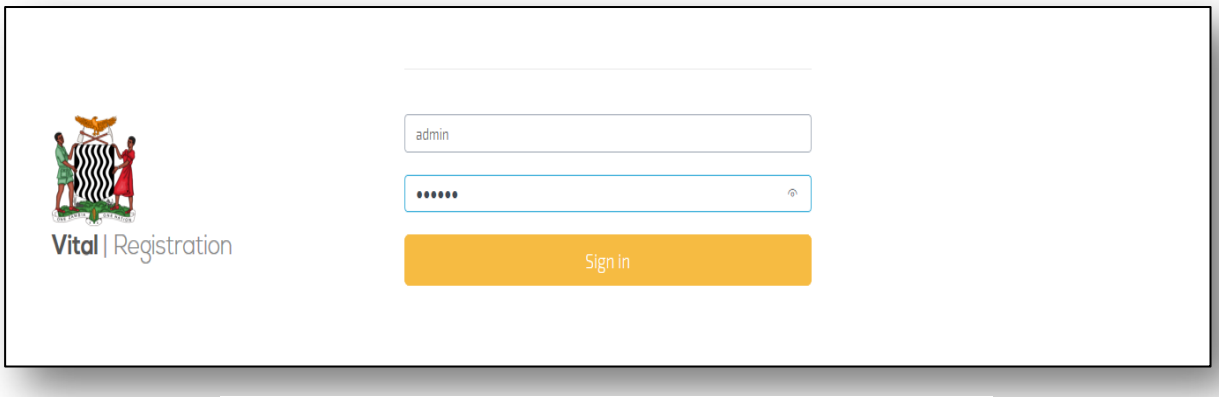


Figure 3.22. Civil Registration system – masked Input

Figure 3.23 shows a full login with the administrator credentials. As can be seen on the left panel of the screen, '*create users'* is displayed on this screen. Menu options are dislayed on the left panel and read '*birth records, generate Vital Document, Registered Identities, Record Template, create users and logout'*.

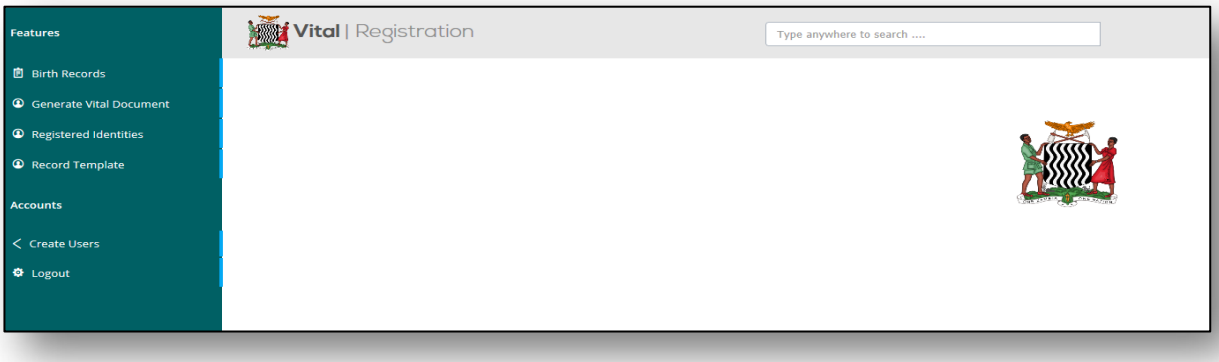


Figure 3.23. Civil Registration system – Administrator Screen

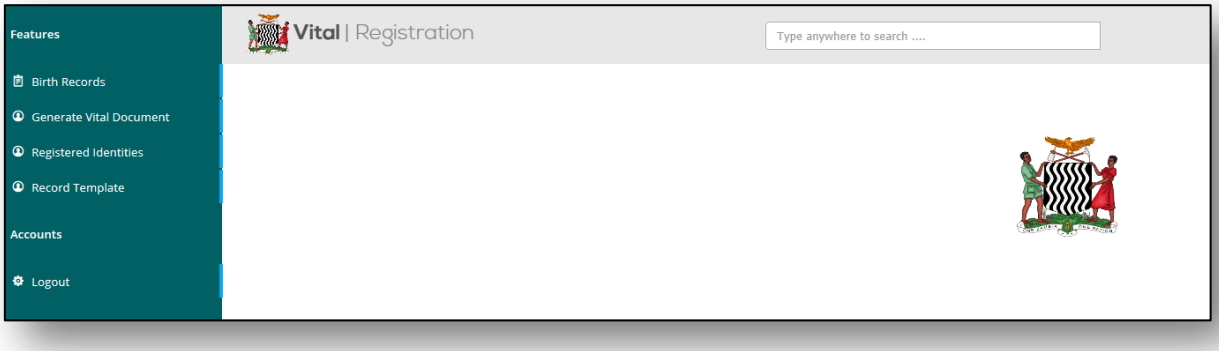


Figure 3.24. Civil Registration system – Sub-User Screen

Figure 3.24 shows a full login with sub-user credentials. The screen can be seen not to display the '*create user'* option. Menu options are dislayed on the left panel and read '*birth records, generate Vital Document, Registered Identities, Record Template and logout.'*

3.5 System Requirement Specifications

Object-Oriented Systems Analysis (OOSA) was used in this study to define the system requirements during the specifications phase [144] [146] [145]. Five elements of OOSA where entered into during the systems development of the civil registration model. These are:

I. The requirements model which aimed to capture the functional requirements of the system [146] [145];
II. The analysis model which aimed to give the civil registration system a healthy and changeable object structure [144];

III. The design model that aimed to refine the object structure to the current implementation environment [146] [145];
IV. The implementation model which aimed at implementing the system [144]and
V. The test model which aimed at verifying that the system operated as planned [146].

System requirements are a definition of what a system is capable of doing through provision of a service. The software object developed to meet a need must be a structure that reflects the situation in which the need arises [146] [145]. Systems requirements are equally meant to define the system constraints. These are the limitations a system faces in its effort to provide its expected services [146]. Systems requirements divide into two i.e.: functional and non-functional requirements. Functional requirements are statements of services provided by the system and how the system is intended to respond to inputs and its response in certain circumstances [145].

The system requirements specifications for the civil registration system gives an overview of all the functionalities and specifications for the proposed model [145]. The civil registration system is developed to comprise eight modules namely: '*Administrator, Sub-user, Authentication, Birth Details, Bio-Capture, Bio-Calibrator, Bio-Recognizer, and Report'* as shown in the component diagram [145] [144] in Figure 3.25. Component diagrams are used to show what the various modules in the systems are and not to show any interaction among those components [144] [145].

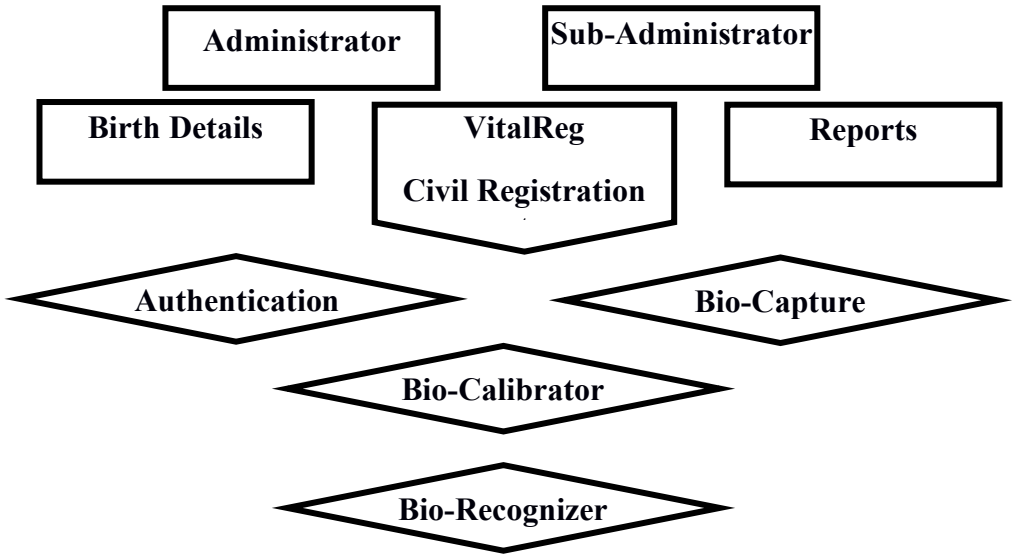


Figure 3.25. Civil Registration system Component Diagram – System Modules. Adapted from [144]

3.5.1 Functional Requirements

Table 3.1: details the functional requirements required for all the modules for the civil registration system.

Table 3.1: Functional requirements

FR 1	The system administrator shall create the new system user
FR 2	The system administrator shall be the super user and will have all the privileges for the entire system
FR 3	The system administrator shall have capacity to appraise user database
FR 4	The system administrator shall generate log files, backup and recovery files for the system
FR 5	Sub-User shall have relevant access rights to enroll a citizen
FR 6	Sub-User shall have relevant access rights to generate and print output documents
FR 7	Sub-User can calibrate biometric data
FR 8	Sub-User can perform authentication
FR 9	All sub-user activities can be performed by a an Administrator User

3.3.3.2 Non-functional requirements

Non-functional requirements are specifications that define a criteria that can be used to judge operations of a system [146]. Table 3.2 details the non-functional requirements required for all the modules found in the civil registration system.

Table 3.2: Non-functional requirements

NFR1	The system shall be easily maintainable in case of requiring forwarding criteria changes without stopping the whole system
NFR 2	The system failure shall not affect data integrity
NFR 3	All software application modules shall be debugged
NFR 4	The system shall be faster when multi-core central processing are used
NFR 5	The software system and application code shall be well documented, and this will be written in a familiar language
NFR 6	The system shall provide the documentation that shall have all functionality and any user maintenance for the system administrators

3.5.2 System modelling and design

3.5.3 Introduction of unified modelling language (UML) diagrams

This section illustrates the use of the unified modelling languages (UML) which has been used to visualize, state, create and document the dynamic aspect of the system in diagrammatic form. These diagrams illustrate the behavior of the system at differing levels of operation and in certain instances at levels of abstraction [146] [154] [145]. The diagrams are categorized as follows: Use case diagrams, interaction diagrams and activity diagrams.

3.5.4 Use case diagrams

Use case diagrams are used to exemplify the arrangement of tasks that a system undertakes to determine a result. It is a diagram that specifies the entire functionality of the system [144]. Interactions that objects take with other objects within the system are also illustrated by use case diagrams and in this way show the abstraction of the system and to some extent the instantiation of objects within the system [145] [146] [154]. Use Case diagrams utilize an object referred to as an actor which is an object that represents functions or roles that users of a use case perform. An actor may imply an individual such as a MoHA interviewer or an entity such as a computer. In certain cases, an actor may represent a system such as the University of Zambia. Table 3.3 explains the USE CASEs found in the system.

Table 3.3: USE Case Explanations for the Civil Registration System

Actor	Description
MoHA Citizen Registration Officer (Sub-User)	Undertakes all activities of enrolling a citizen into the citizen registration system.
Village Authority (sub-user)	The entity that can access the citizen system to print out a record of birth template.
Citizen	The individual who is the subject of enrolment into the civil registration system.
Administrator	The administrator is the super user of the system and shall have all the privileges for the system.
Haar Cascade Classifier	It is responsible for providing various functions of biometric analysis for the system.

Figure 3.26 shows the diagrammatic representation of the actors and the respective use cases for the civil registration system. Table 3.4 provides an explanation of the USE CASEs used in Figure 3.26.

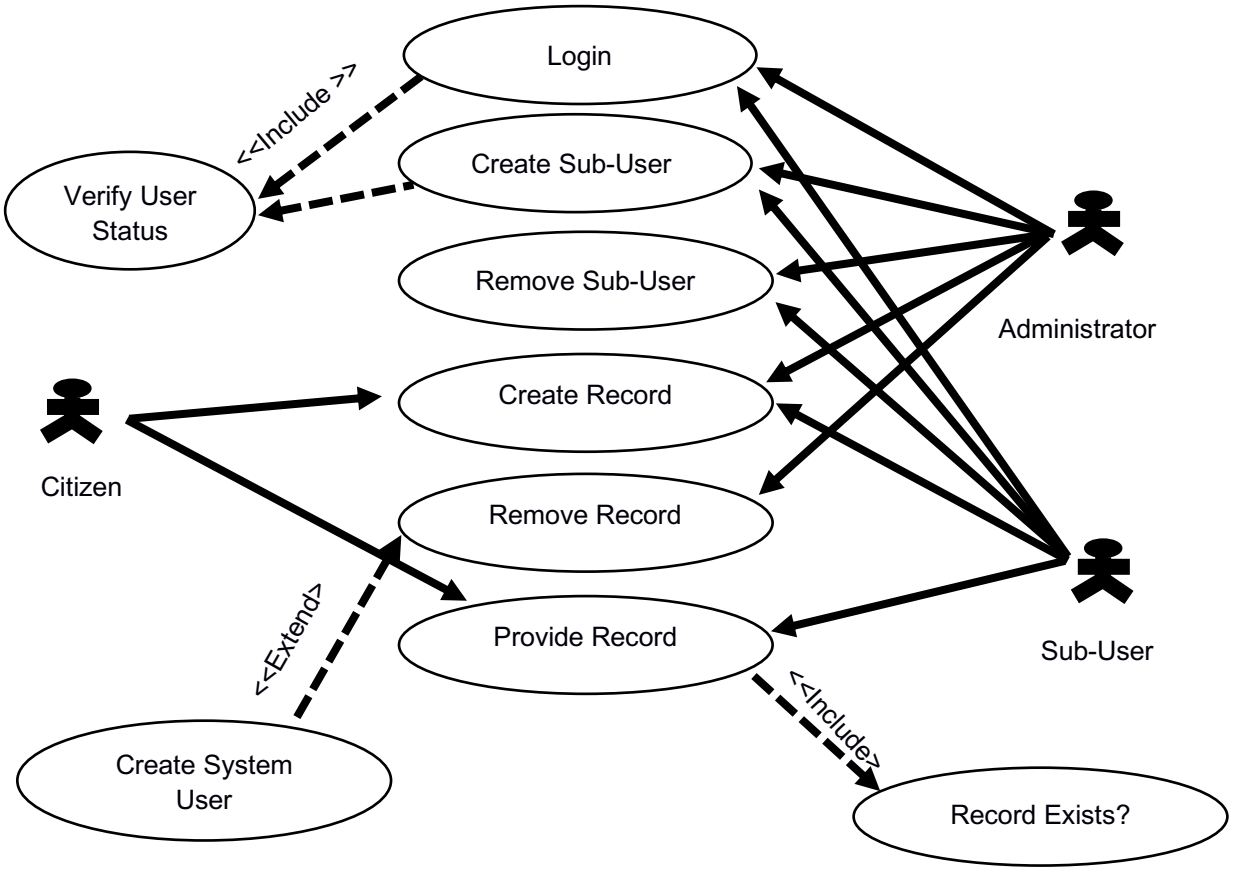


Figure 3.26. Civil Registration System – Use Case

Table 3.4: Description of Figure 3.26 use case diagram

Actor	Description
Login	Allows a registered user on the system to login to the system
Create Sub-User	Allows the administrator to add users to the system. Allows a sub user access to the system
Remove Sub-User	Allows the Administrator to remove users from the system. Denies access to a removed sub-user
Create Record	Allows a registered user to enrol a citizen onto the system
Remove Record	Allows the administrator to destruct a citizen record
Provide Record	Allows a citizen to provide personal data, allows a registered user to enrol a citizen

Figure 3.27 shows the various interactions of the actors and Use Cases that shall be involved in the user application interface of the Civil Registration application system. Actors are: Administrator/ Registrar General (Super / System User), Registration Officer (Sub-User), Citizen.

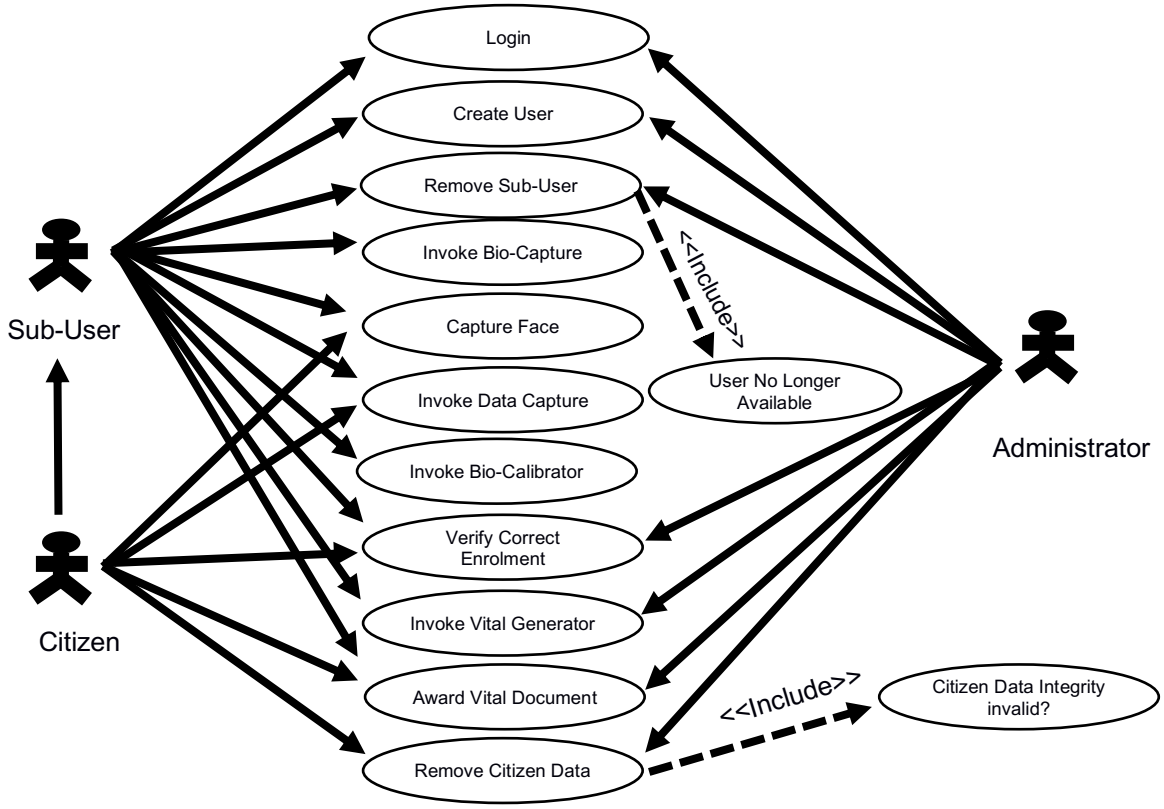


Figure 3.27. Civil Registration system – Use Case Interactions at User Interface Level

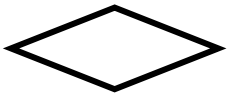
3.5.5 Interaction models – Activity and sequence diagrams

3.5.6 Activity diagrams

Activity diagrams comprise of a set of events or actions that are connected together by transitions or changes from one activity to the next. Activity diagrams make it easy to demonstrate the three structural elements of all procedural languages used in computer programming or software engineering namely: sequence, selection and iteration [145] [146] [144] [154]. The possibility of capturing the elements of programming are an advantage in that modelling and communication of business processes in a particular system becomes easy.

Notation of activity diagrams [154] is illustrated in Table 3.5:

Table 3.5: Activity Diagram Notation. Adapted from [154]

Symbol	Description
	Activity of Process or single action or behaviour
	Begin or initiate or start node
	Termination or final activity node or Stop
	Note or construct
	Decision point or selection
	Object flow
	control flow or transition

3.5.7 Interaction Sequence diagrams

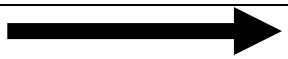
Use cases stipulate the processes that are required to undertake a user task. The user tasks may involve a number of interactions between a number of different objects [144] [146]. As an illustration from the civil registration system to print a NRC will affect the QR Code Mapper module and the Geospatial module plus the encryption module. These mentioned objects then interact by sending each other messages. The various systems objects then respond to these messages by implementing methods [145].

Methods themselves are an implementation of an operation [146]. Interaction Sequence or Sequence diagrams show these interactions.

Sequence diagrams evolve as the systems development progresses.

Table 3.6 for illustrates the symbols used in interaction sequence diagrams.

Table 3.6: Sequence Diagram Notation. Adapted from [146]

Symbol	Description
	Actor
	Activation
	Object Life
	Message
	Object symbol
	Message return
	Object message

In this section, the details for the activity and interaction sequence diagrams for each use case in Table 3.4 will be described.

A) Login

Figure 3.28 details how the login module of the civil registration systems' login user interface (UI) is invoked by instantiating the object '*vitalReg'* (Figure 3.20). VitalReg passes control to the login module that invokes a user prompt that requests the user to provide the system with their system credentials needed to access the other aspects of the civil registration system. These credentials are passed on to the authentication module for user authentication. The authentication object requests the user details from the user database and performs a match for correctness of details. Should the credentials match the database details as held then access is awarded to the user to access the Civil Registration System Desktop.

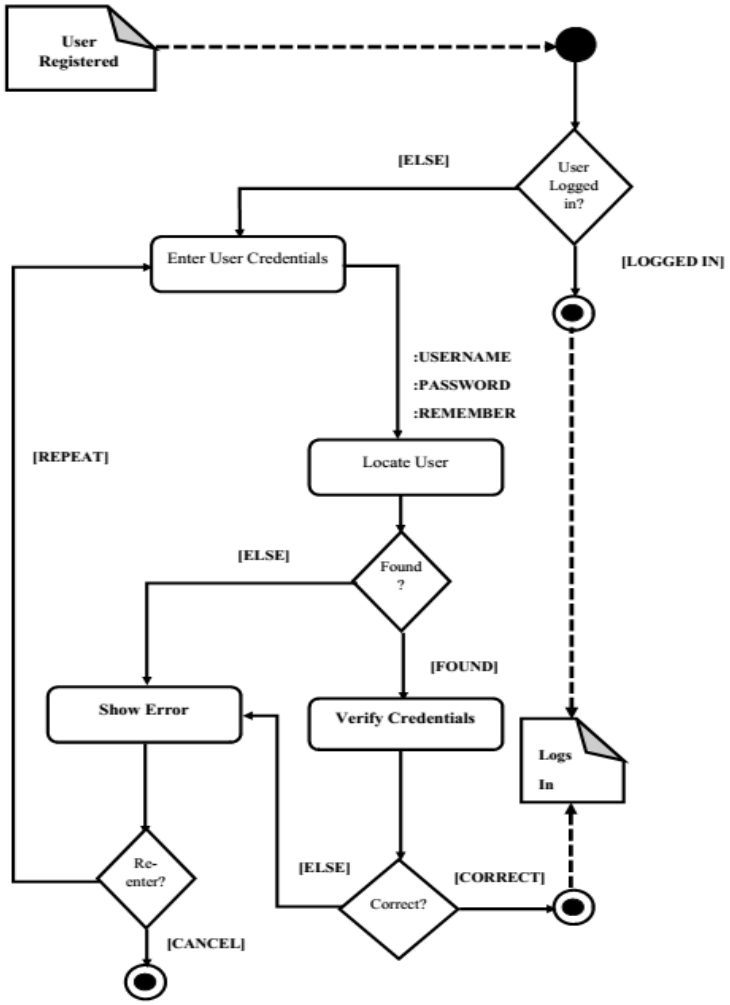


Figure 3.28. Civil Registration system – Login Activity Diagram

The sequence diagram in Figure 3.29 details the sequenced operation illustrated in Figure 3.28 concerning the login module.

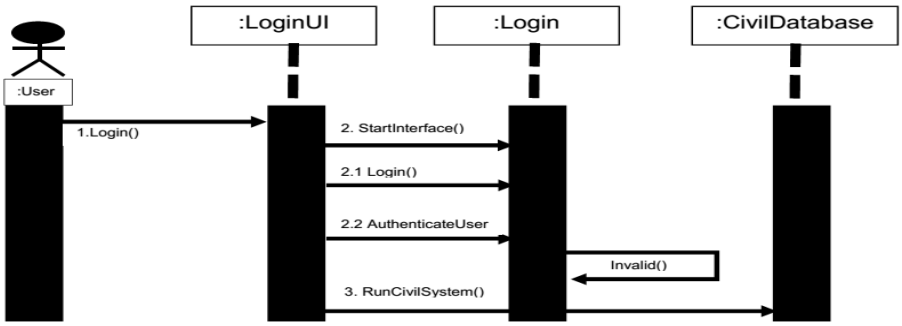


Figure 3.29. Civil Registration system – Sequence Diagram

B) Remove User and Remove Citizen Data

The administrator must be logged into the system server for this operation to be successful. The administrator will invoke the '*phpMyAdmin'* area of the system and manually remove user details. The process of data removal is left this way because the author believes the concept of security by obscurity will suffice [155]. Figures 3.30 and 3.31 illustrate the sequence and activity diagram for this task respectively.

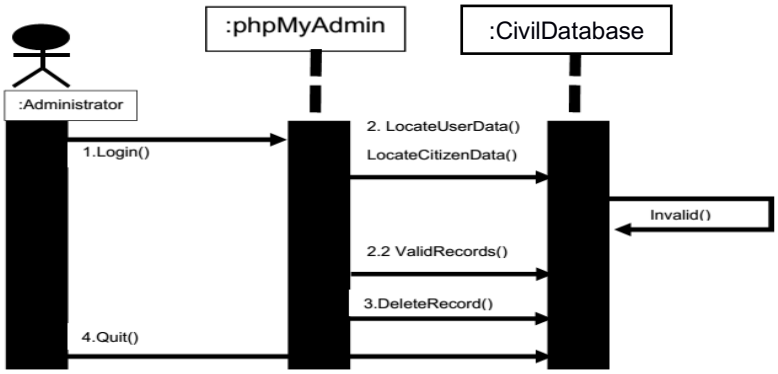


Figure 3.30. Civil Registration system – Remove User and Citizen Data Sequence Diagram

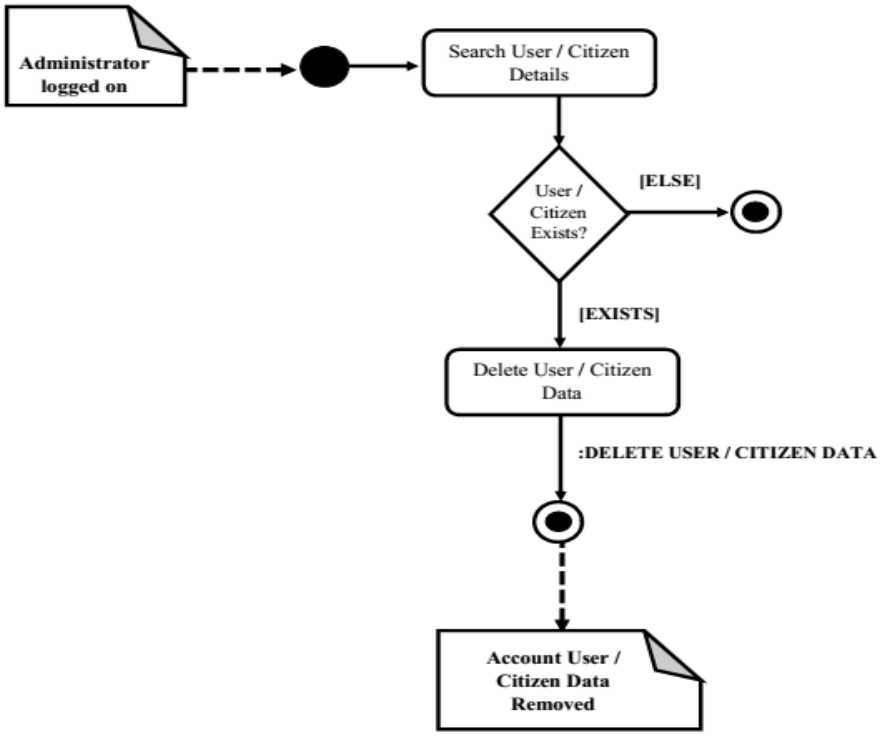


Figure 3.31. Civil Registration system – Remove User and Citizen Data Activity Diagram

C) Invoke BioCapture

Figure 3.32 shows the activities undertaken in the invoke BioCapture module of the civil registration system. The module activates an object that runs the camera hardware, detects a face on the camera and captures multiple images of that face (100 to be specific) and saves the images.

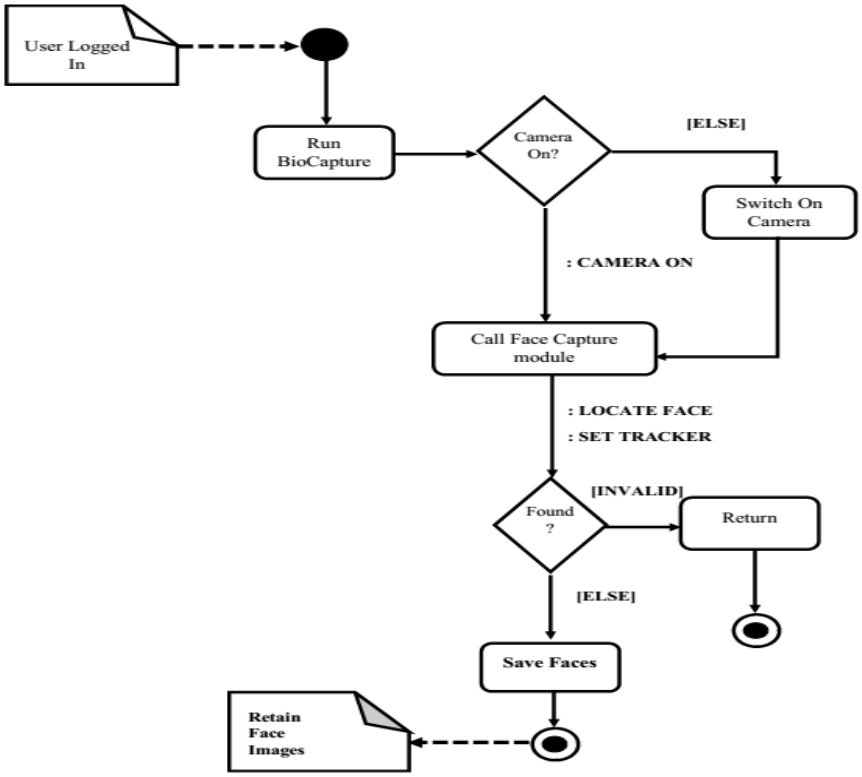


Figure 3.32. Civil Registration system – Invoke BioCapture Activity Diagram

Figure 3.33 is the collaborating sequence diagram for the activity diagram shown in Figure 3.32.

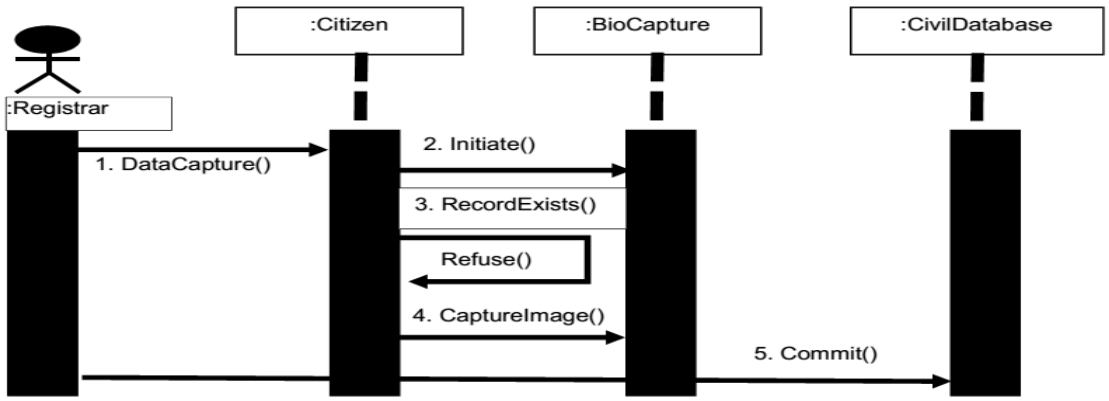


Figure 3.33. Civil Registration system – Invoke BioCapture Sequence Diagram

D) Invoke BioCalibrator

The BioCalibrator module is responsible for the generation of a strong classifier from the weak classifier that result from the images captured from the BioCapture module. This object is instantiated by the object calibrate which in turn is run by the event calibrate from the desktop panel of the civil registration system. Figure 3.34 illustrates the activity diagram.

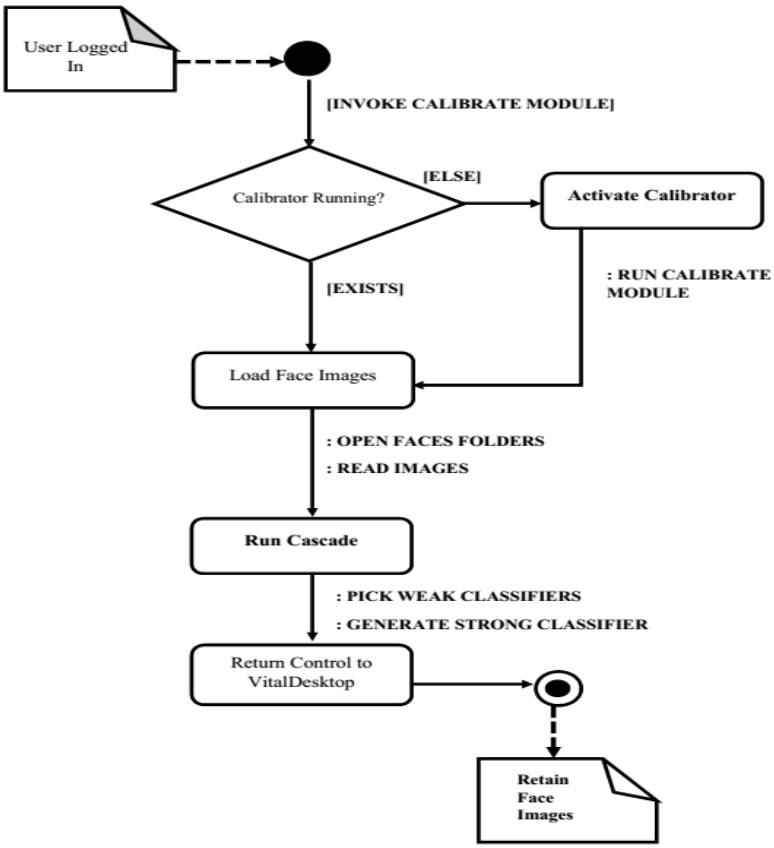


Figure 3.34. Civil Registration system – Invoke BioCalibrator Activity Diagram

Figure 3.35 illustrates the sequence diagram for Figure 3.34 Invoke BioCalibrator module.

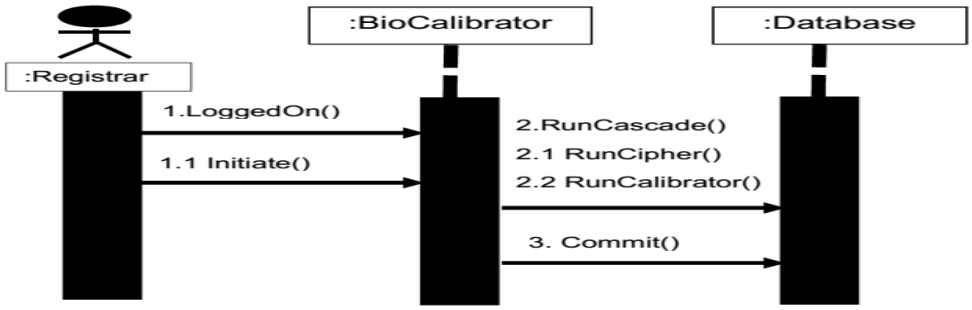


Figure 3.35. Civil Registration system – Invoke BioCalibrator Sequence Diagram

E) Verify Correct Enrolment (Verifier / BioRecognizer)

Figure 3.36 shows the activities undertaken by the BioRecognizer or Verifier object module of the civil registration system. The object module has one function to compare the earlier enrolled facial images' Haar-like features against the current image placed on the camera. The object must then prompt the system user of its finding. The finding can be a positive match or a negative match. In certain cases, either FRR or FAR might be recorded depending on environment setting and image placement.

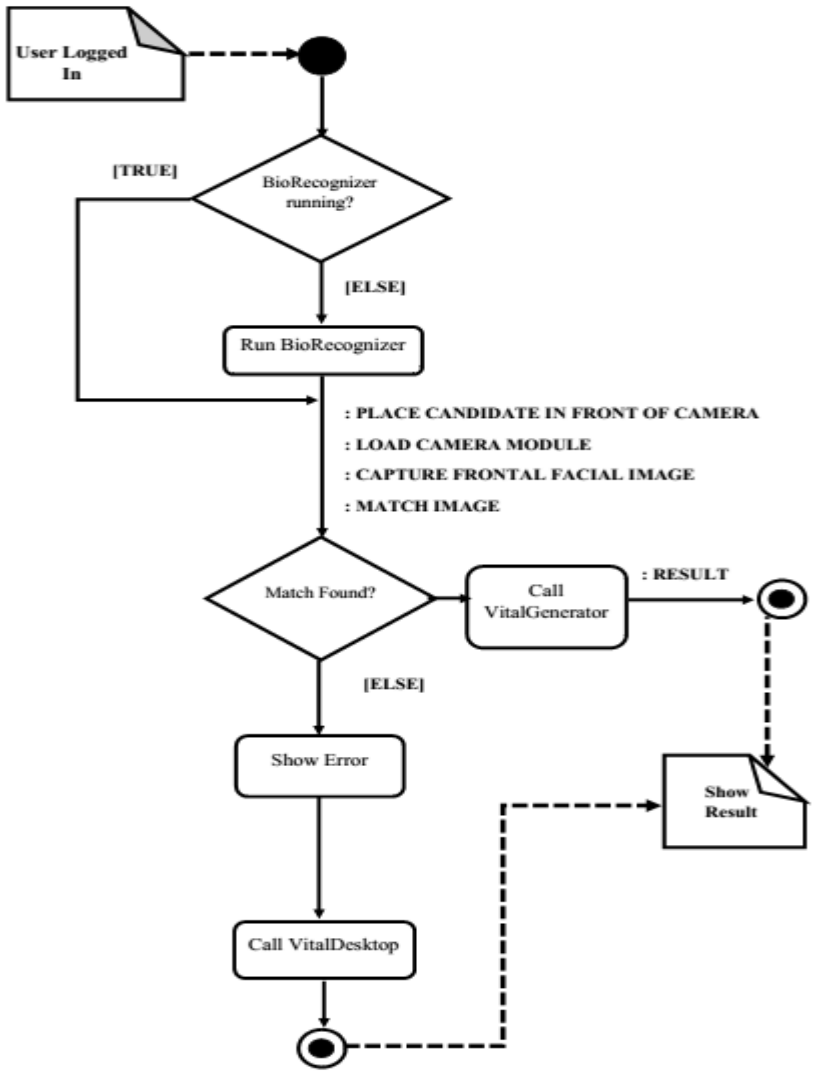


Figure 3.36. Civil Registration system – Invoke BioRecognizer / Verifier Activity Diagram

Figure 3.37 shows the corresponding sequence diagram for the BioRecognizer object module.

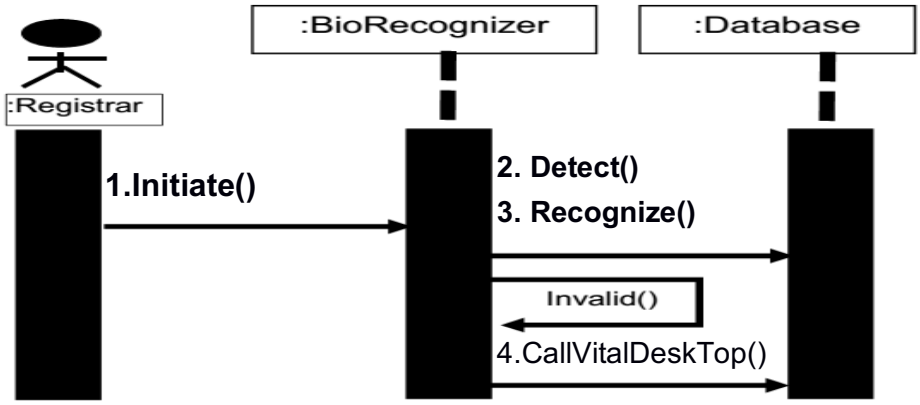


Figure 3.37. Civil Registration system – Invoke BioRecognizer / Verifier Sequence Diagram

F) Invoke Vital Generator

Figure 3.38 illustrates the activities that are undertaken in the generation of a vital document.

To perform these operations, a user must be logged in and the details of the citizen must exist on the civil database.

A verification must have been run as shown in Figure 3.36 and confirms that that citizen data is existent on the civil database. This module instantiates the verifier which runs the object BioRecognizer (Verifier, see Figure 3.36) object that performs a match of a face available on the camera to its strong classifier as defined by the BioCalibrator. If a match is positive, the object options for Birth Certificate and NRC are made available with the captured facial image of the citizen. The vital desktop at this point instantiates the object module QRCode Mapper which generates the QR Code from birth certificate number, date, name and sex of the citizen. The Geospatial Mapper is equally launched here to place the GPS coordinates of the registration center carrying out the registration.

Once complete, the final documents requested either NRC or Birth Certificate can then be printed. Figure 3.39 illustrates the sequence diagram for the activities in Figure 3.38.

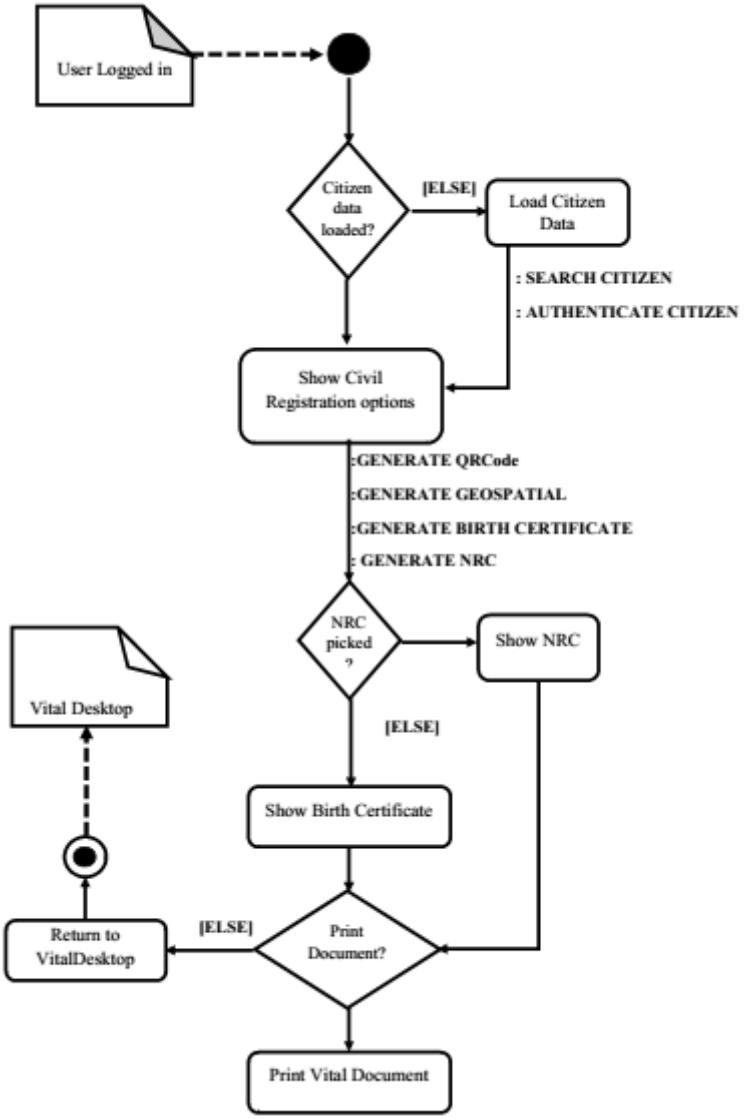


Figure 3.38. Civil Registration system – Vital Generator Activity Diagram

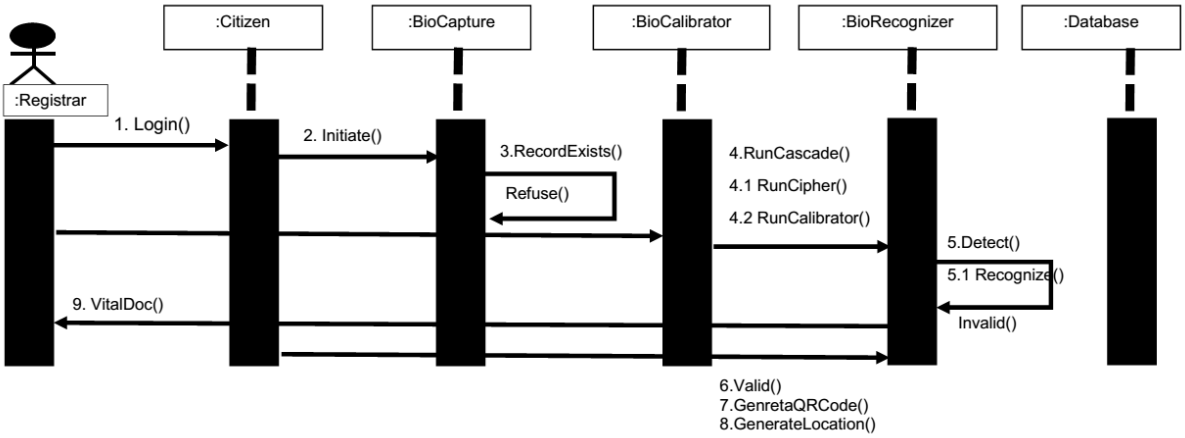


Figure 3.39. Civil Registration system – Vital Generator Sequence Diagram

G) Create User

Figure 3.40 shows the Create User module object of the civil registration system. This module is launched by the object module create from the vital desktop user interface (UI). Once launched the object module instantiates a data collection window that allows for user data to be collected and retains this information into the user database. User detail collected includes usernames, passwords that can be used to grant access to that registered user. This module is only available to the administrators of the civil registration system. Figures 3.40 and 3.41 illustrate.

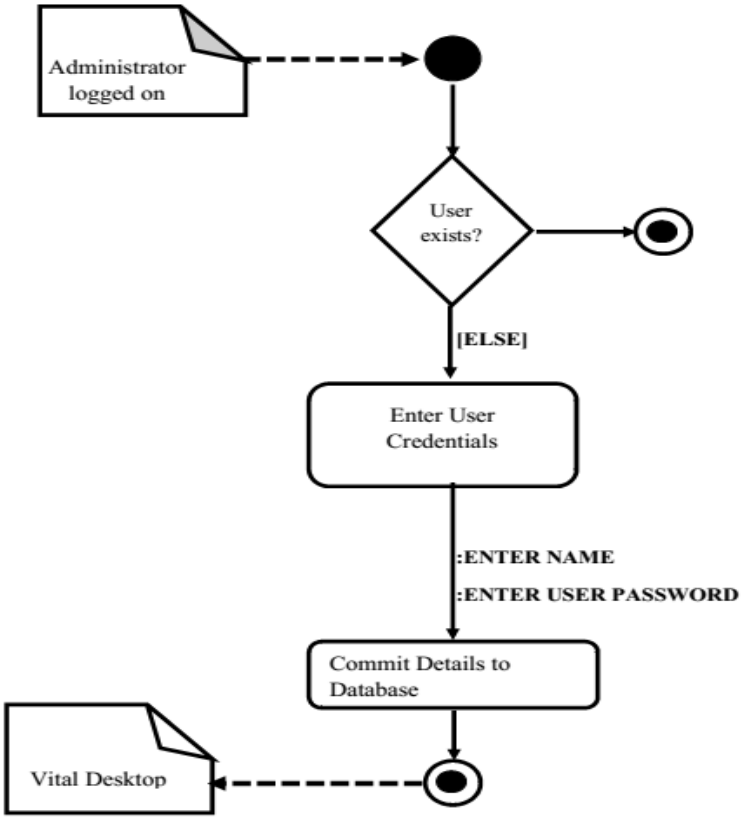


Figure 3.40. Civil Registration system – Create User Activity Diagram

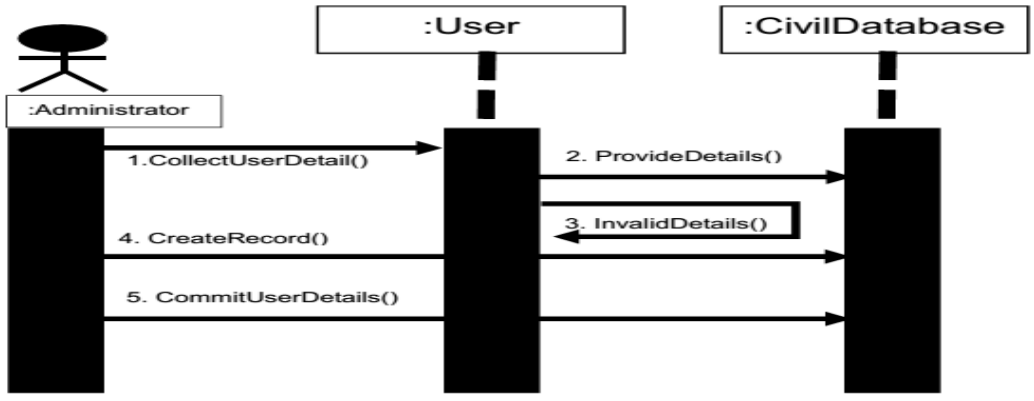


Figure 3.41. Civil Registration system – Create User Sequence Diagram

3.5.8 Logical Data Structures – ERM and Class diagrams

In order to organize the basic classes and objects into a hierarchies that enable the benefits of inheritance to be realized logical data structures are used. Several UML diagrams are used to achieve this. Diagrams that can be used include the UML Class diagram and UML ERM diagram [145] [146] [144]. In order to understand the mechanics of logical data structures several concepts must be understood as follows [146]:

i. Inheritance is the mechanism by which an object implements an association or relationship of abstraction of common elements and specialization between classes;
ii. A class is a container of similar objects and an object is an entity that has capability to retain information and may offer operations or messages. It is a concept in an application domain that can be represented as an encapsulation of state, behavior and identity;
iii. Encapsulation itself is the hiding of internal information or modes of operations of an object or a class and
iv. An entity is a representation of a class. Entities may be physical elements.

3.5.9 Notation of UML Class Diagrams

Class diagrams use the following notation as shown in Figure 3.42:

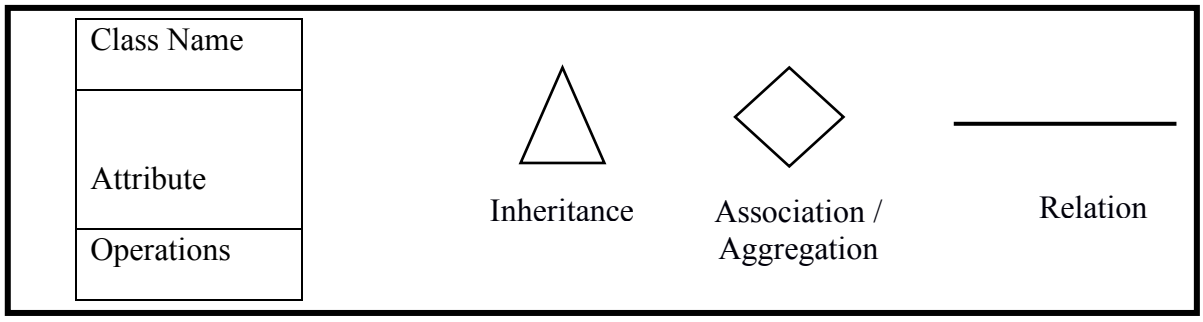


Figure 3.42. Class Diagram Notation. Adapted from [145] [146] [144]

Figure 3.43 shows the UML Class diagram for the civil registration system. The Class diagram is drawn to the specifications as shown in Figure 3.42 and houses the relationships and attributes of each tuple in the database. Relationships and associations are equally shown. As can be seen, the civil database has 4 tuples in its' database named as follows:

i. *birth_certs* housing all the data on birth certificates, which has its' primary key set to '*id* 'and has an auto increment setting added to generate an id number in an incremental fashion;

ii. The *'authentication'* tuple housing the details on the valid authenticated details about a citizen. These details are placed in here once a strong classifier has been generated. The primary key in here is the '*id'* which has the settings equivalent to the birth_Certs' '*id*' field. The secondary key here is the '*birth_id';*

iii. The '*user*' tuple which houses the details about the various systems users. The primary key here is the *'id' and*

iv. The '*birth_details'* housing the details about the birth details of an individual. The primary and secondary keys are '*id'* and '*birth_id*' respectively.

The primary and secondary keys provide the various relations needed to transport data to and from the tuples.

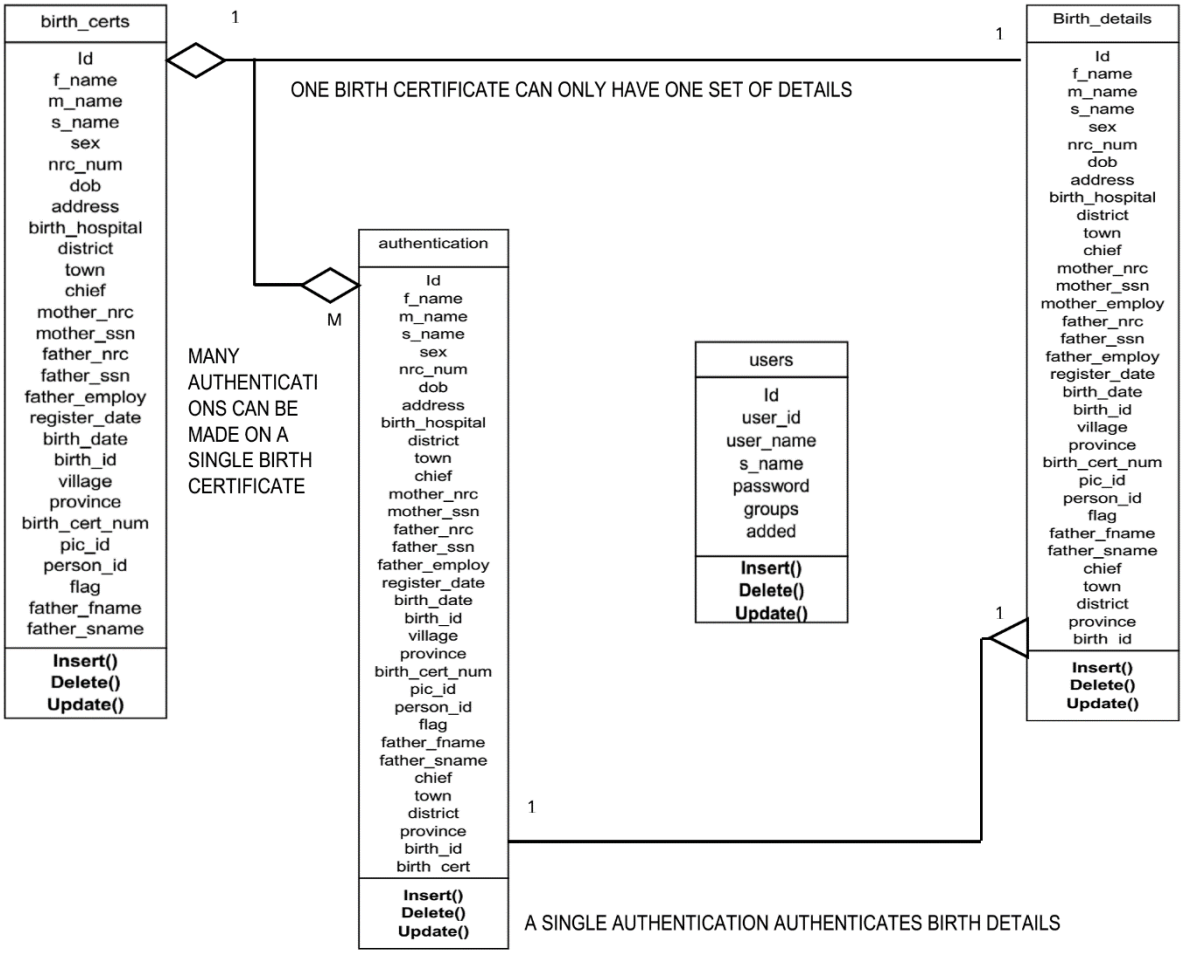


Figure 3.43. Civil Registration system – UML CLASS diagram with entity relation modelling

3.6 System Implementation

The database has been developed using MySQL. The prototype has been developed using php, HTML, JavaScript, python, CSS, batch files and uses the XAMPP control panel to manage the server abilities on standalone computing resources. The facial detection and recognition algorithm (haar-cascade) uses XML. Within-person variation can be taken into account through a non-generative approach earlier discussed in section 2.7.3.

All the software kits that have been used are open source applications and are readily available on the internet at no charge.

3.7 Limitation of the Prototype

The civil registration system is limited to few trials. Due to this fact, the application may NOT match the functions expected in industry processes. Access, finance and time are two factors that impeded the full test in either live-test or dry-run with civil registration centers. Time factor alone limited the development process to what is represented in the component diagram in Figure 3.25.

3.8 Summary

This chapter has utilised results from the baseline study. The problems that were identified generated a basis for which a civil registration system was designed and developed to mitigate the problem of easier and secure civil registration that yields a vital document in the name of a birth certificate and NRC. The use of biometrics to run civil registration systems provides convenience, gives a sense of a better service delivery by GRZ, in particular the MoHA.

CHAPTER 4

RESULTS

4.1 Introduction

This chapter presents results collected from the baseline study and results of implementation of the civil registration system. The baseline results are presented in such a way that they cover the views of the research participants. The research participants included: ICT regulators, Standardization bodies, Consumer protection authorities, students in higher education institutions, banks, Government Ministries and departments, Health Support Institutions and general users. The results of the system implementation is done through the use of screen shots of the civil registration system operations.

4.2 Research Participant Responses

4.2.1 Introduction

In Zambia, The Ministry of Home Affairs is headquartered in Lusaka. It is by association that the head office is expected to run the Civil Registration System. A total of 18 organisations were sampled in the study with each organisation providing a minimum of 4 research participants. The Ministry of Home affairs – directorate for civil registration and passport office provided valuable insight into the civil registration processes. The author presents research findings for the research participants based on their: general information, knowledge on biometrics, knowledge on regulation concerning biometrics and their opinion on storage and management of biometric data. The presentation of the results is in form of tables, bar-charts and pie-charts.

4.2.1.1. Overall Research Participant Occupation Status

Because the study was aiming at providing a solution concerning a civil registration system that utilizes human PII through biometrics and a biometric system, it was necessary to determine the occupation status of the of research participants. This was helpful because the organizations that were purposively sampled all collected PII at one stage or another in their line of work.

Figure 4.1 shows the overall occupation status of the research participants. It can be seen that 37 of participants are in the subordinate position, 33 are in the managerial position, 21 are in the supervisory position, 5 are in the directorial position and finally 4 are in the executive position.

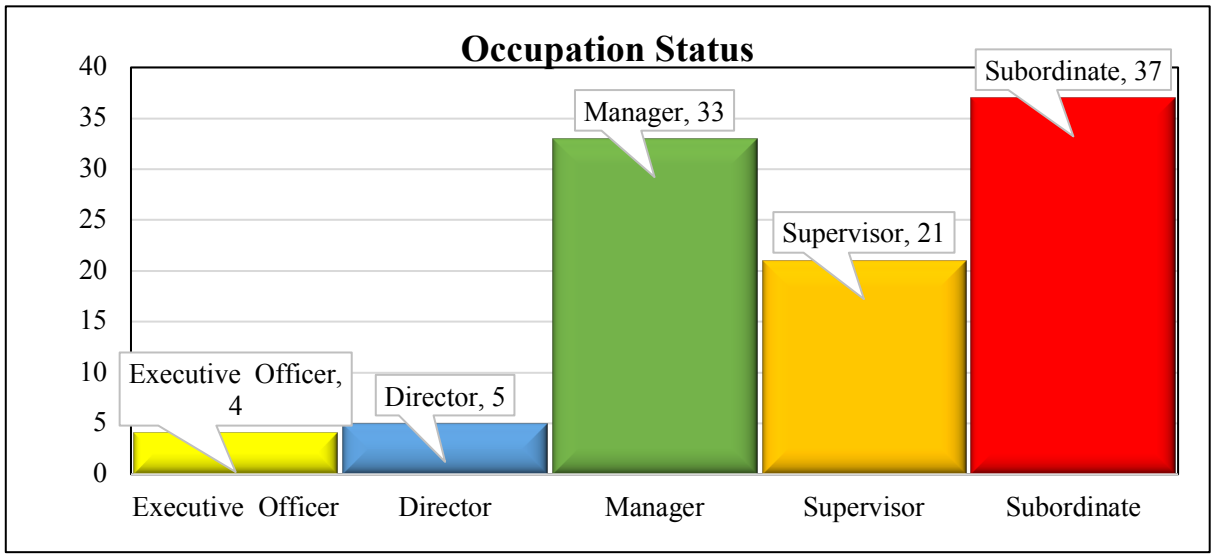


Figure 4.1. Civil Registration Survey – Participants' Occupation Status

4.2.1.2 Biometrics and Public Perception

We illustrate the general understanding that the research participants hold concerning biometrics. The idea here is to show how the public views biometrics and biometric systems in terms of functions biometrics and biometric systems perform, how biometric data may be managed, how the research participants understand the various biometric systems implemented at their institutions of work and how they view or understand the various interventions GRZ introduces in the management of biometrics and biometric data. A pie-chart was used to describe the results of the participants relating to whether they had ever heard of or had any knowledge or were aware about biometrics. Figure 4.2 shows that the larger percentage of the participants (88%) specified that they were aware or had some knowledge concerning biometrics.

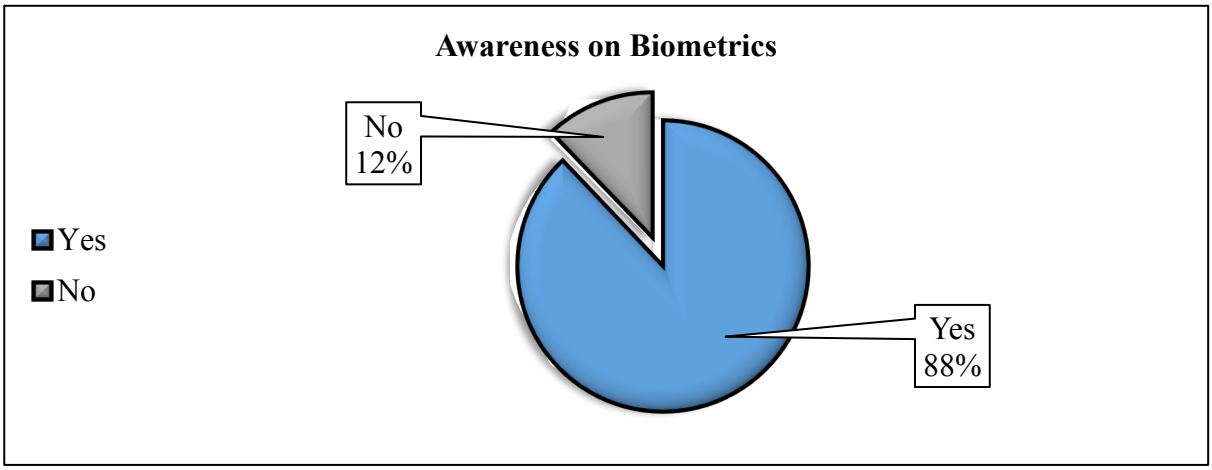


Figure 4.2. Civil Registration Survey – Participants' awareness concerning biometrics

4.2.1.3 Source of knowledge on Biometric

Research participants were asked as to whether they had any knowledge of the kind of work biometrics perform. Figure 4.3 shows the outcome of this query. Participant response was parameterized to Radio, TV, Internet and Friends. Participants were required to pick from these options as their source of information to answer the question. To ensure all possible answers could be captured the questionnaire had an open ended response labeled *"Others, Specify . . . ."* which allowed for any answer other than the ones given. Figure 45 illustrates.

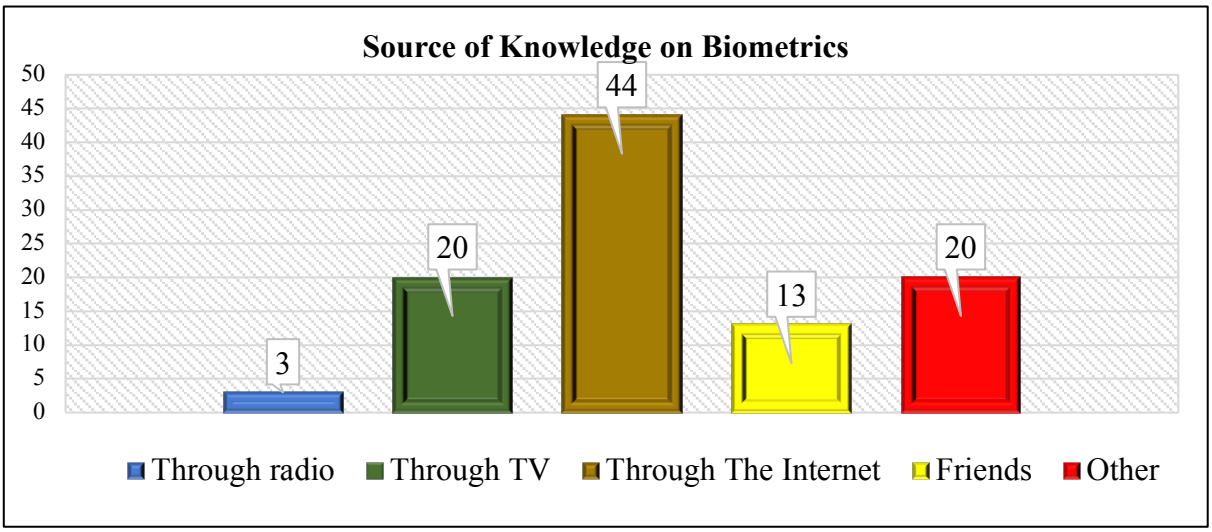


Figure 4.3. Civil Registration Survey – Participants' awareness concerning biometrics

4.2.1.4 Organisations that utilise a biometric data usage framework

Figure 4.4 shows a doughnut pie-chart which was used to describe the results of participants whose Organisation utilized a biometric framework to supervise the usage of biometric data that is collected in the Organisation. The majority 66% stated heir Organisation did not implement such a framework, 26% claimed their Organisation had such a framework and 8% could not provide any answer to this question

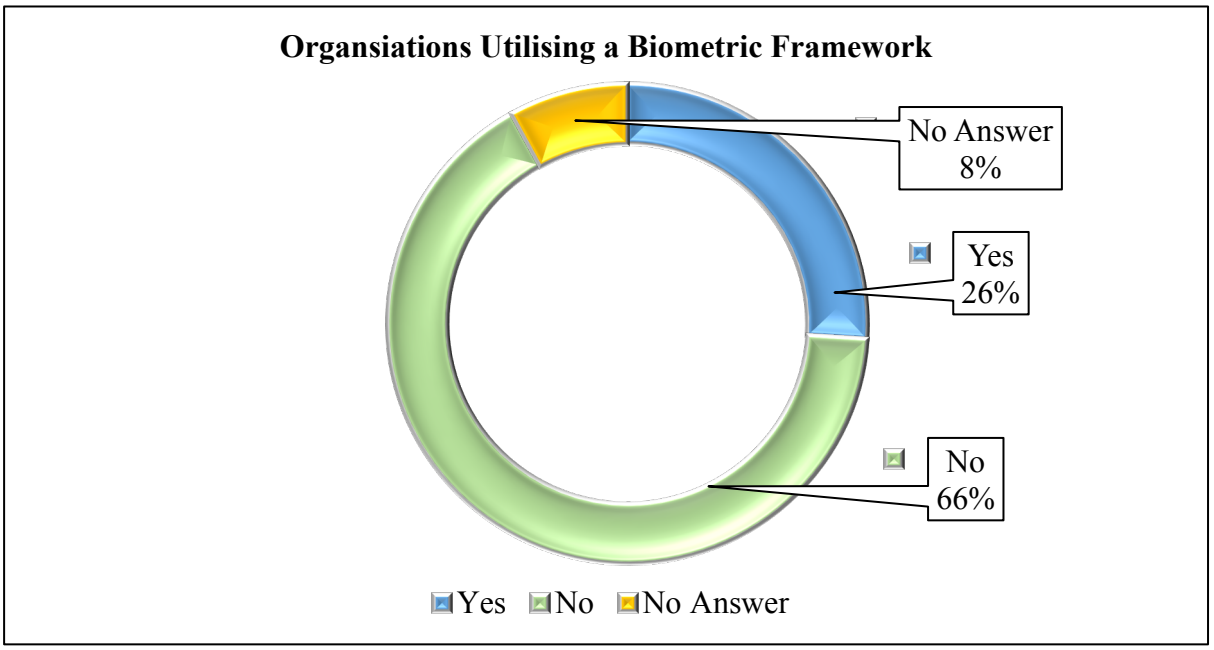


Figure 4.4. Civil Registration Survey – Organisations with biometric framework

4.2.1.5 Location of One's Biometric Data

The participants were requested to state where they thought their biometric data collected from them should be stored. As can be seen in figure 4.5 stated that this data must be kept somewhere at their work places while the other 50% were divided between the Internet at 16% and others at 34%. The others in this case believe that the GRZ offices, physical files, NRC centers, MoHA, papers Cloud servers, secured servers should store the biometric data. Others simply were not sure of what was expected of them. 0% of the participants felt their data could be stored at their CEO's residence.

Figure 4.5 demonstrates these findings.

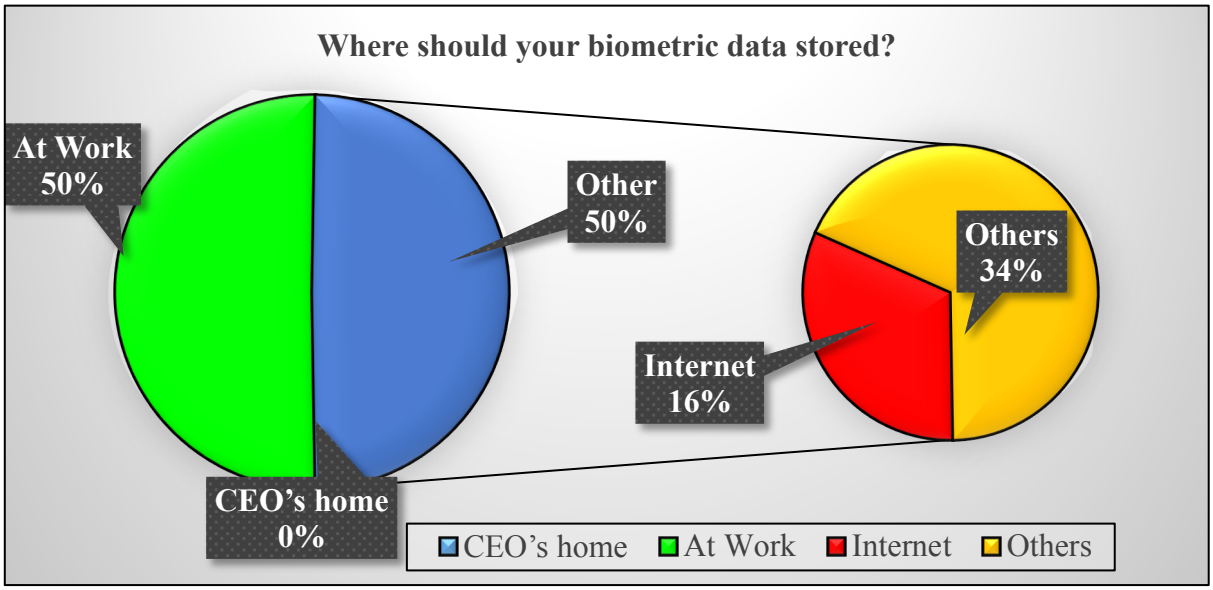


Figure 4.5. Civil Registration Survey – Participants' view of where biometric data should be kept

4.2.1.6 Work Biometrics Perform

Figure 4.6 shows the various responses from the research participants concerning what they thought biometrics and biometric data perform within the ICT ecosystem. 46% stated that biometrics are used to provide information security services, 20% criminal services, 12% Government statistics, 19% medical services and 3% others. The others in this case could not state what they believe biometrics perform.

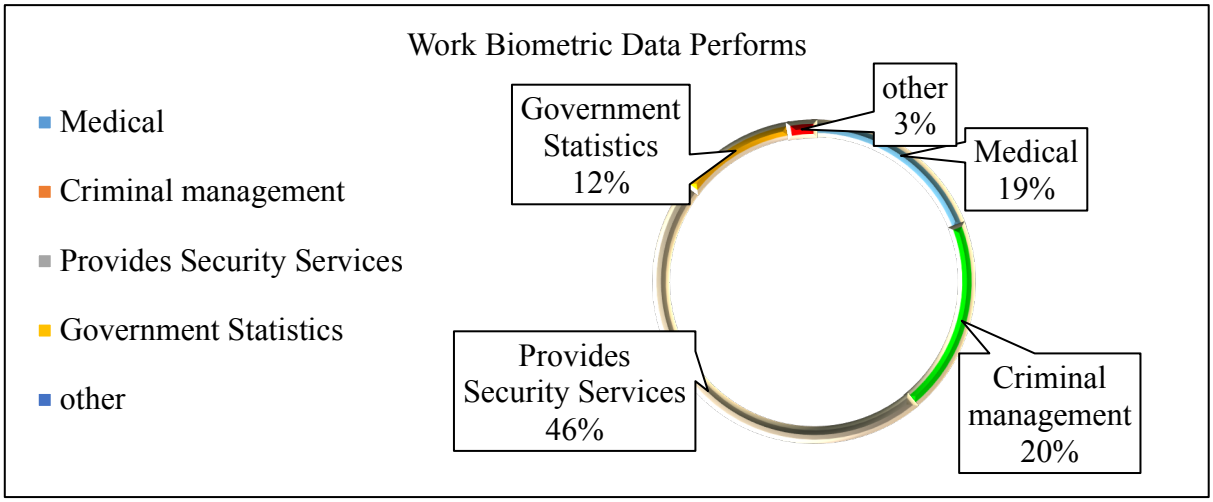


Figure 4.6. Civil Registration Survey – Work Biometrics Performs

4.2.1.7 Awareness on Government Innovations Concerning Biometrics

Figure 4.7 shows that responses from 98 participants indicate that they have no knowledge of any ZICTA or GRZ innovation to manage biometric data. 1 research participant, however stated that they were aware of GRZ or ZICTA innovations to manage biometric data in Zambia. 1 individual could not provide any answer to this question.

This question was also extended to include a section of explanation of the type of innovation if mentioned that the participant was referring to. The individual who respondent in affirmative in this section COULD HOWEVER NOT PROVIDE a response further than "INGRIS".

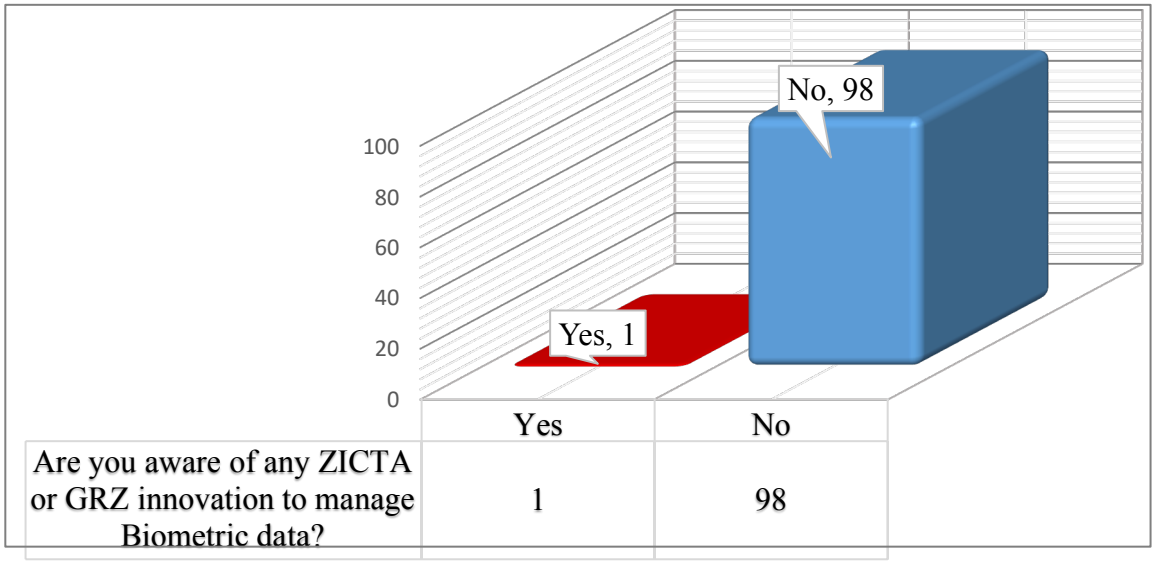


Figure 4.7. Civil Registration Survey – Awareness to GRZ/ZICTA innovation on biometrics

The participants were also expected to state what issues the GRZ or ZICTA can implement in order to improve on their role in facilitating development through ICTs in Zambia. The response to this question was overwhelmingly 'sensitization' at various levels starting with school curriculum.

4.3 Likert Scale Type Responses

In this section we demonstrate the various answers that the research participants provided to a number of questions that probed their attitude towards biometric data usage. Participants

were expected to provide an answer which showed how they strongly felt about an issue by providing a response which was scaled to a range of 1 to 5. One (1) in this scale showed the strongest felt response while 5 showed the least strongly felt response.

The grading was then analyzed by Microsoft Excel quantitatively. A framework of the expected responses now follows:

For each of the following statements circle one of the options to indicate how you feel. The options are labelled 1 - 5.

SA = Strongly agree (with statement)	1
A = Agree (with statement)	2
N = Neither agree or disagree (with statement)	3
D = Disagree (with statement)	4
SD = Strongly disagree (with statement)	5

4.3.1 Support for the Use of Biometric Data

Figure 4.8 shows the responses to the question probing research participants on their support for their biometric data to be used for organizational information security based on 6 factors namely: awareness, user needs, expectations, perception and attitude. Table 4.1 shows the tabular form of the results presented in Figure 4.8.

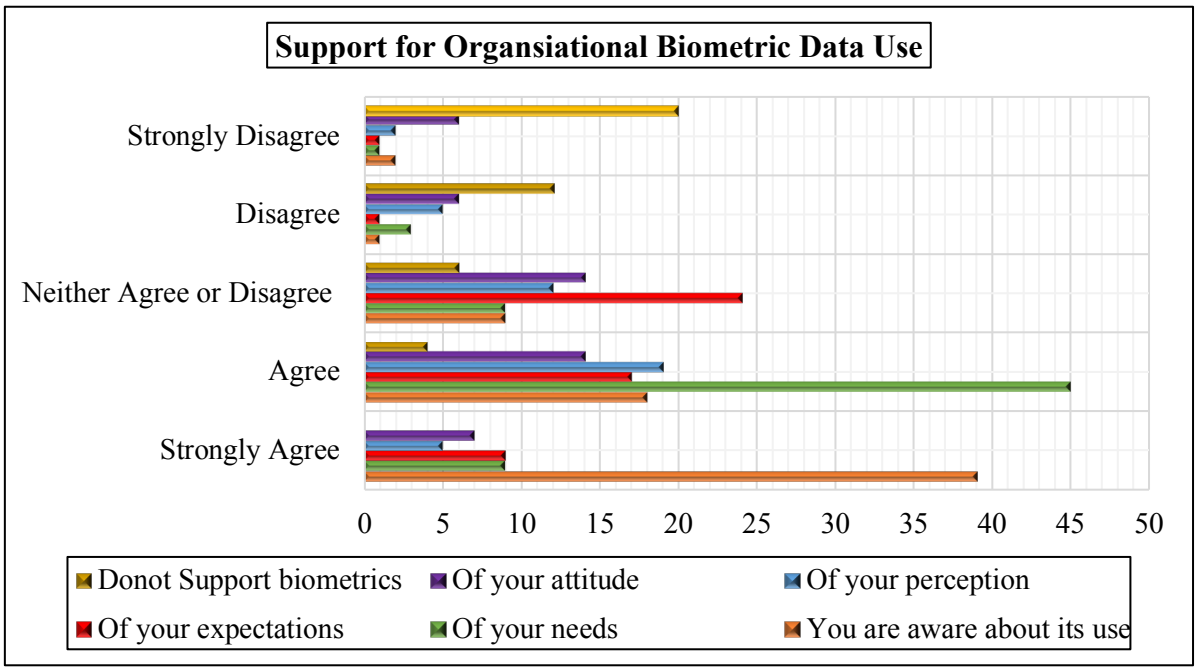


Figure 4.8. Civil Registration Survey – Support for use of biometric data

Table 4.1: Civil Registration Survey – Support for use of biometric data

Support for USE OF YOUR BIOMETRIC DATA for organisation information security objectives because					
	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
You are aware about its use	39	18	9	1	2
Of your needs	9	45	9	3	1
Of your expectations	9	17	24	1	1
Of your perception	5	19	12	5	2
Of your attitude	7	14	14	6	6
Do not Support biometrics	0	4	6	12	20

4.3.2 Storage framework for biometric data for the Zambian Environment.

Figure 4.9 shows the various responses that the research participants provided to the question seeking their responses to the query asking them to state whether ZICTA must develop a framework to supervise the use of biometric data in Zambia. Table 4.2 is the corresponding tabular information relating to Figure 4.9.

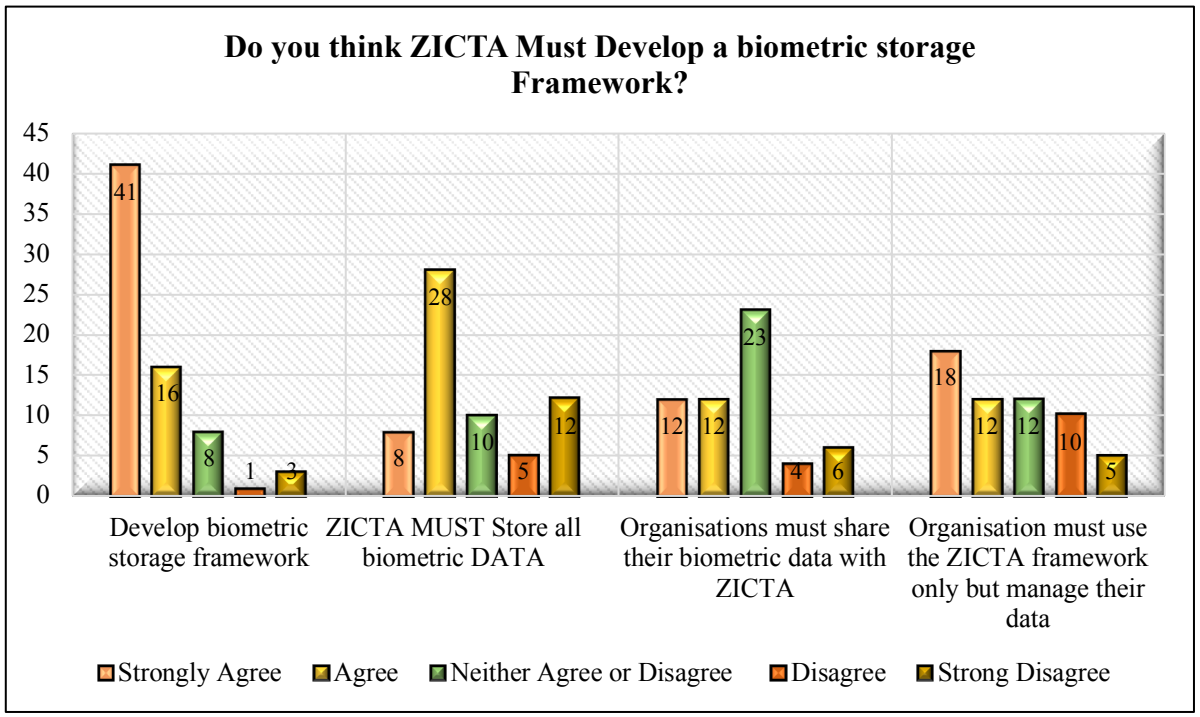


Figure 4.9. Civil Registration Survey – ZICTA must develop a biometric Storage framework

Table 4.2: Civil Registration Survey – Biometric storage model

ZICTA must Develop Biometric storage model					
	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strong Disagree
Develop biometric storage framework	41	16	8	1	3
ZICTA MUST Store all biometric DATA	8	28	10	5	12
Organisations must share their biometric data with ZICTA	12	12	23	4	6
Organisation must use the ZICTA framework only but manage their data	18	12	12	10	5

4.3.3 Preference of participants to biometric data storage.

Figure 4.10 shows the responses by the participants to the question enquiring on how they preferred to have their biometric data stored. Table 4.3 corresponds to Figure 4.10.

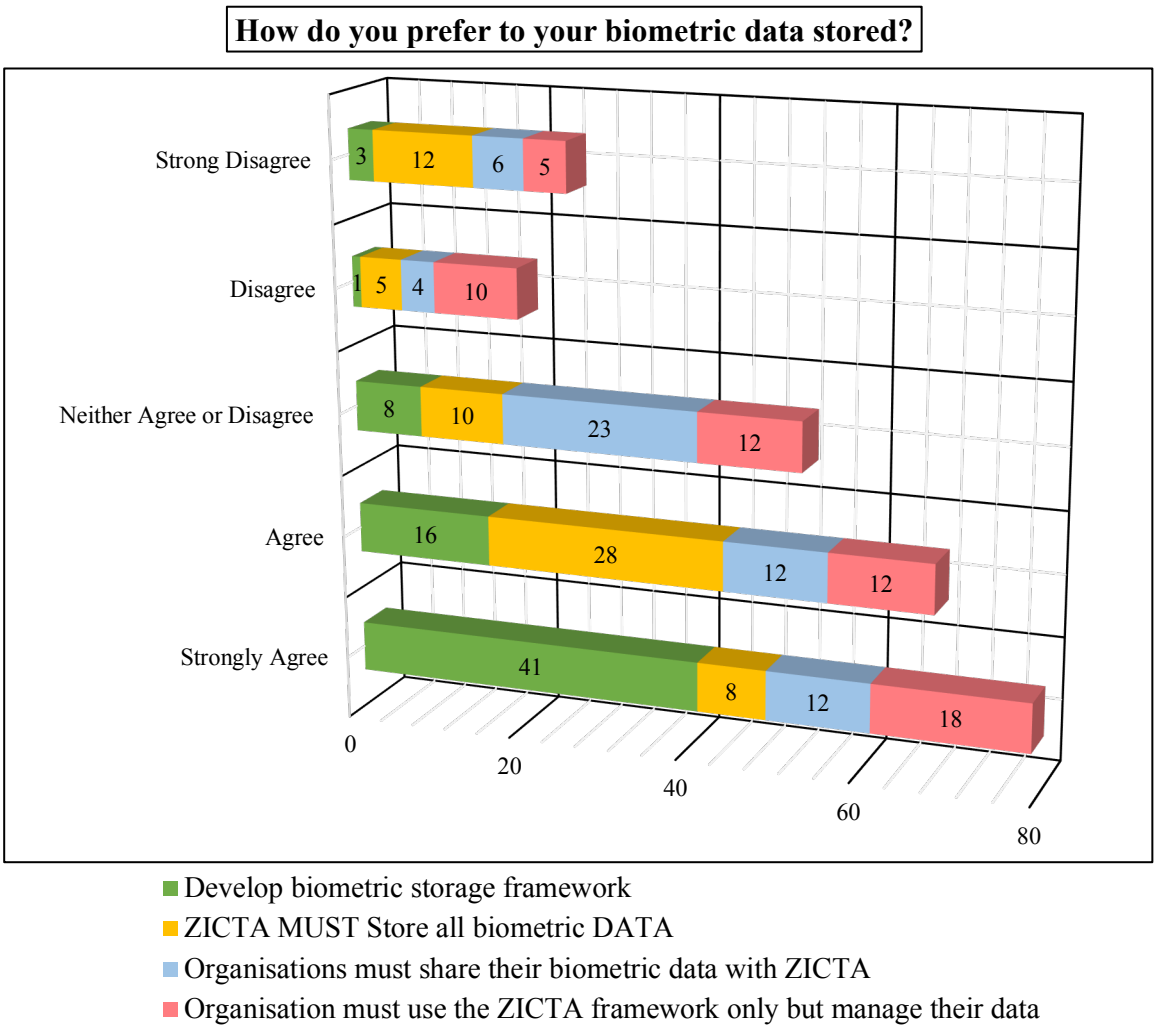


Figure 4.10. Civil Registration Survey – Biometric Storage preference

Table 4.3: Participants preference to biometric data storage

ZICTA must Develop a Biometric storage model					
	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strong Disagree
Develop biometric storage framework	41	16	8	1	3
ZICTA MUST Store all biometric DATA	8	28	10	5	12
Organisations must share their biometric data with ZICTA	12	12	23	4	6
Organisation must use the ZICTA framework only but manage their data	18	12	12	10	5

4.4 Validation

4.4.1 Introduction

In order to ensure this software model we propose can function adequately and meet civil registration processes in Zambia, a validation which is the process of ensuring that a piece of software system or module meets its' systems specification and delivers on its' intent. Aspects of quality control may need to be undertaken to ensure system hoped-for benefits are met [145].

This proposed civil registration system discussed by the author was validated by the IT Specialist Team at DISCOVER Health/SAFE/John Snow Initiative (JSI) Lusaka.

JSI is a non-profit non-governmental organisation which specialises in public health management consulting and research dedicated to improving the health of individuals and communities around the globe. JSI is offering technical expertise to Zambia in the following; Health Systems Strengthening, Monitoring & Evaluation plus others. Among the services JSI is providing to Zambia are Capacity Development, Knowledge Management, applied Technology and Program Development [156]. These services and others imply that JSI is directly involved in assisting the GRZ to meet some of its targets. One of these targets being civil registration. These reasons gave the researchers enough ground to have the Civil Registration System validated with JSI.

The validation process has been undertaken by allowing JSI IT Specialist staff to run the civil Registration system and after which respond to questions set out in questionnaire form.

4.4.2 Validation Results

4.4.2.1 Research Participant Credential

The software validation research participants were initially asked to respond to a question probing their qualifications. The necessity here was to ensure that participants had the know how to respond to validation challenges.

Figure 4.11 indicates the responses to the question referred to above. As can be seen in figure 4.11, of the 6 personal assigned to validate the system, 2 have a Master's Degree, 3 have Undergraduate Degrees and 1 has a Diploma. All these qualifications apart from 1 are within the ICT discipline.

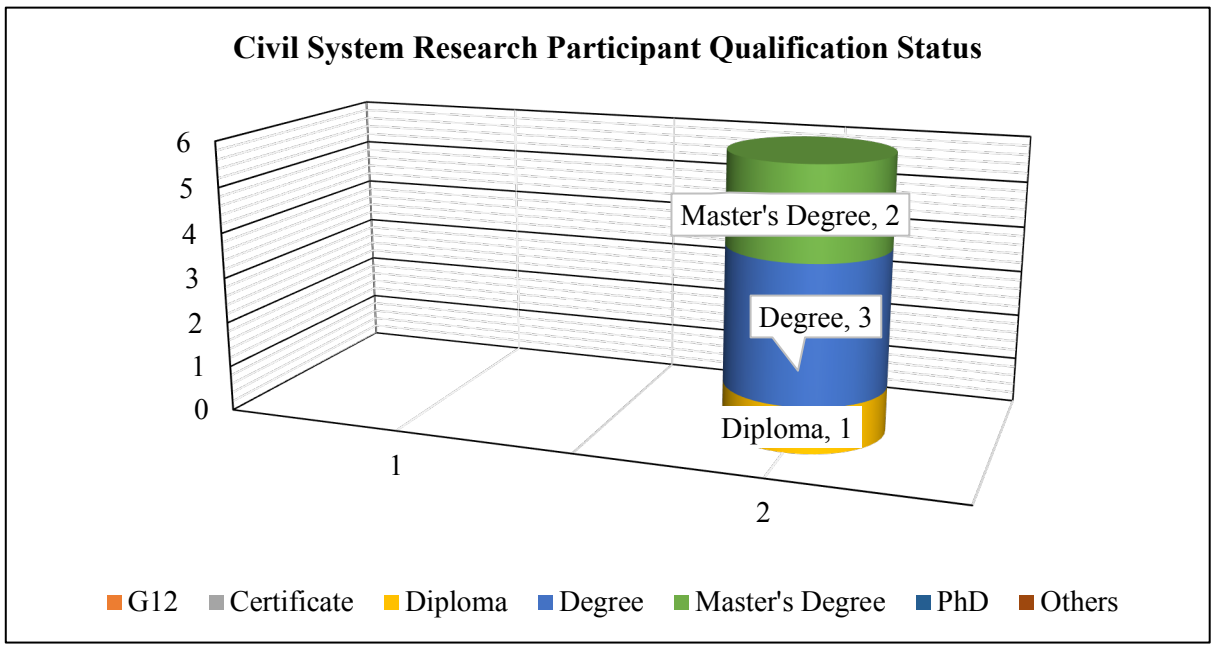


Figure 4.11. Civil Registration System Validation – Participant

4.4.2.2 Research Participant Knowledge

Figure 4.12 shows the responses to the question enquiring on the research participants' knowledge on how to use biometrics. As can be seen all participants responded in the affirmative apart from one.

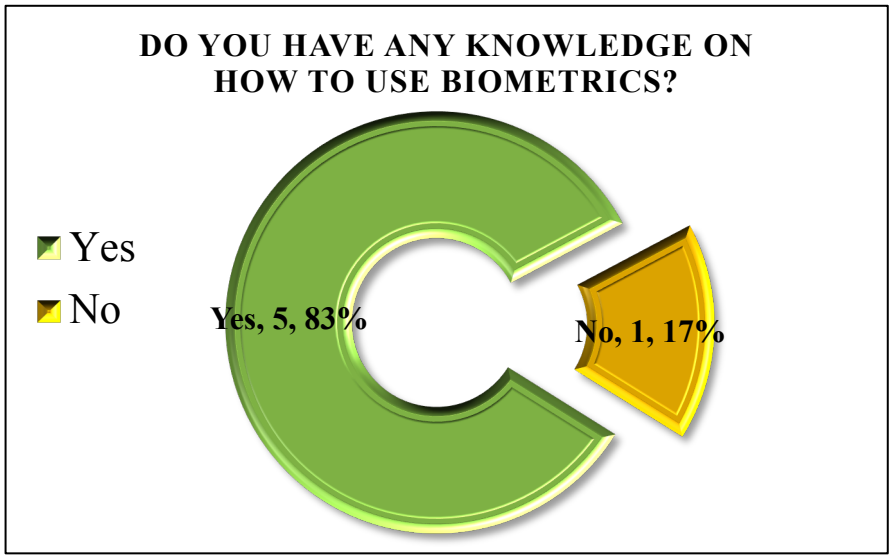


Figure 4.12. Civil Registration System - Participant Knowledge on how to use Biometrics

4.4.2.3 Research Participant Acceptance to Biometric Capture

Research participants were requested to state whether they preferred to have their biometric features captured as a way to initiate validation. Figure 4.13 illustrates the outcome as 4 accepted to this request while the other 2 declined.

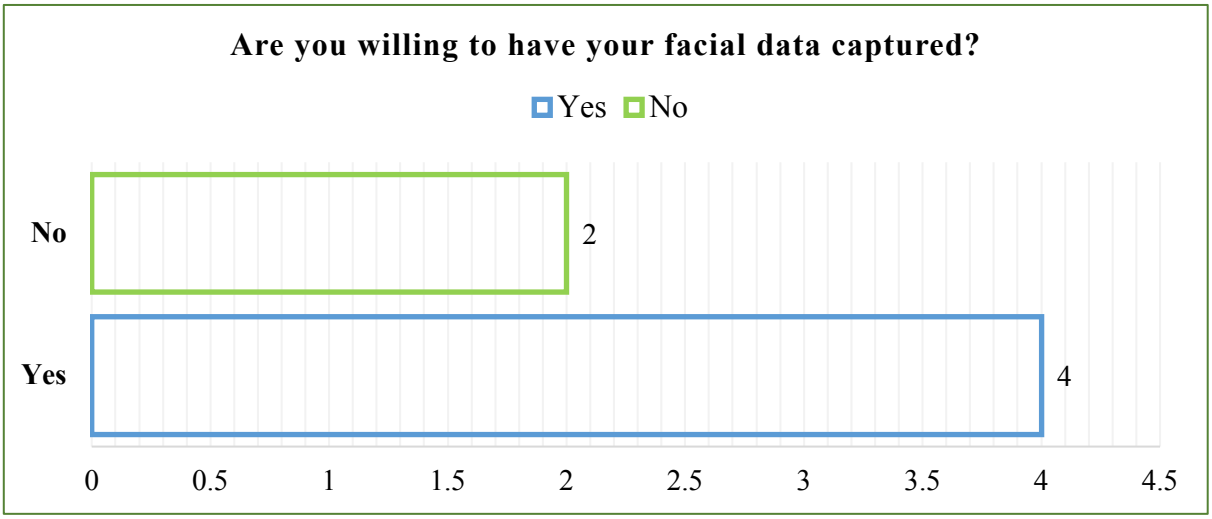


Figure 4.13. Civil Registration System – Response to Biometric Facial Capture

4.4.2.4 System Reliability, Usability, Performance and Portability

4.4.2.5 Learning Curve

Research participants were requested to answer a question probing how the participant viewed the learning curve of using the civil registration system. In Figure 4.14; SA = Strongly Agree, A = Agree; N = Neither Agree nor Disagree; D = Disagree and SD = Strongly Disagree.

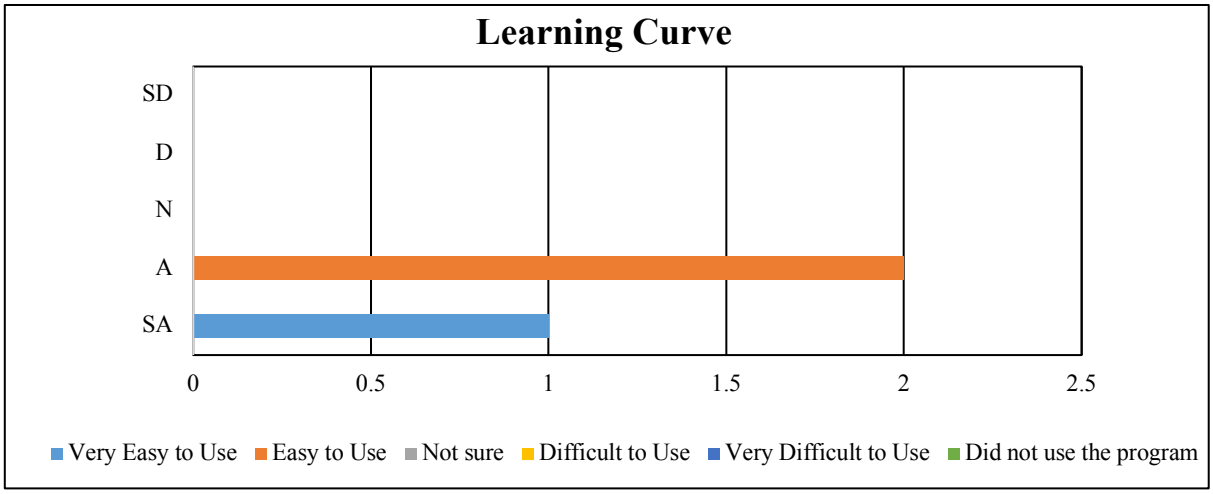


Figure 4.14. Civil Registration System – Learning Curve of System Use

4.4.2.6 Satisfaction of Use

Research participants were requested to state the satisfaction level they obtained from system use of the civil registration system. Figure 4.15 illustrates this result.

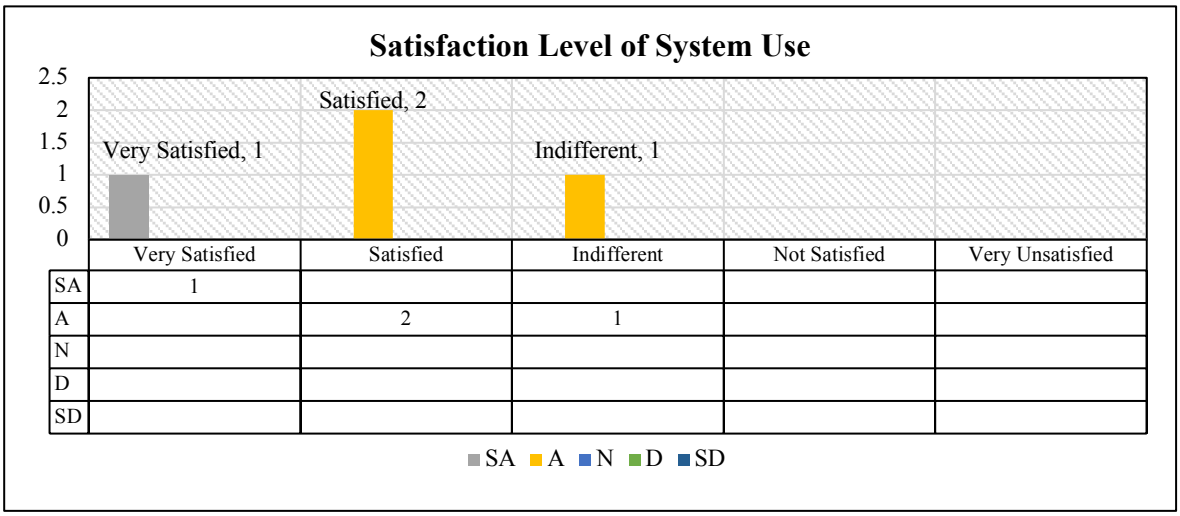


Figure 4.15. Civil Registration System – Participant' Satisfaction Level of System Use

4.4.2.7 Recommendation to use system for Civil Registration Processes

Figure 4.16 shows responses the research participants gave to the question asking them to recommend the civil registration system for civil registration processes in government processes. 2 out of the 6 participants said they would recommend the system, 1 was indifferent, and the other 2 were silent.

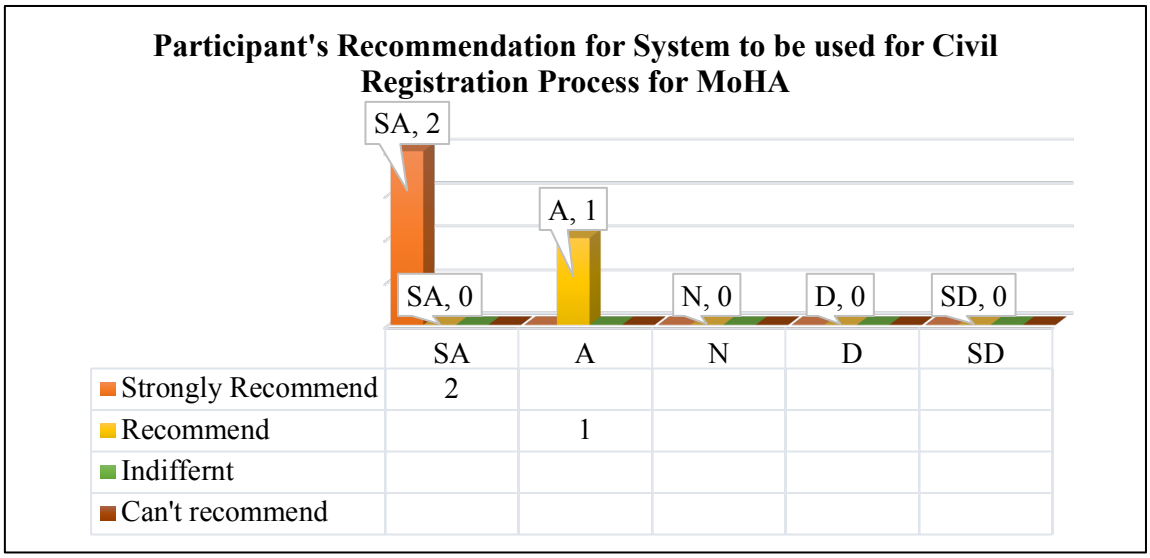


Figure 4.16. Civil Registration System – Participant's Recommendation

4.4.2.8 Interest to use the Civil Registration Processes

Figure 4.17 illustrates the research participant's interest to work with the civil registration system often. As can be seen 2 out of the 6 participants said they would very much be interested to work with the system often, 1 participant held the view that they would like to work with the model while 1 participant was not sure.

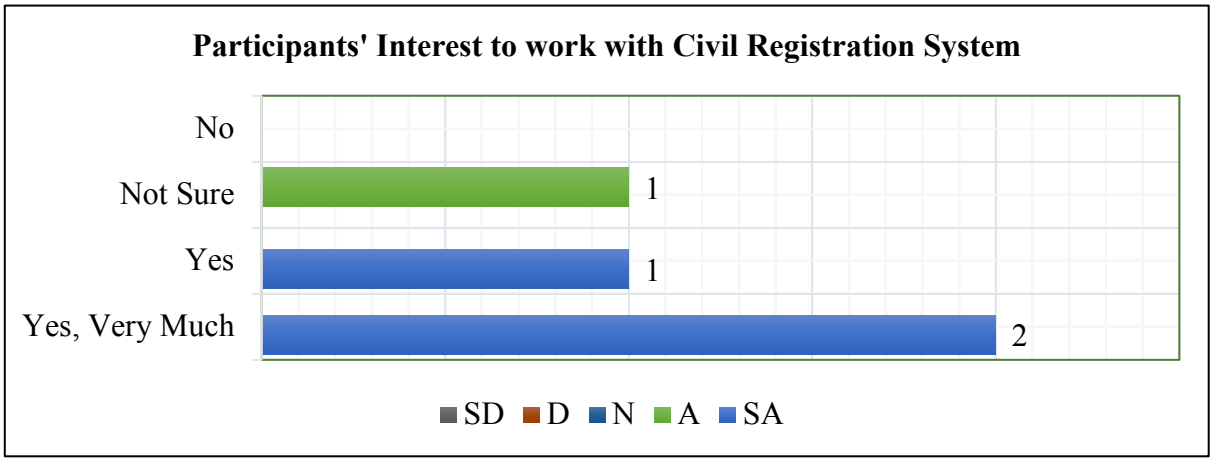


Figure 4.17. Civil Registration System – Participant's Desire to work with System

4.4.2.9 Civil System's Ability to meet Job Function

The research validation participants were requested to comment on how they viewed the system's ability to meet job functions that a civil registration officer would undertake. Figure 4.18 shows that out of the 6 research validation participants

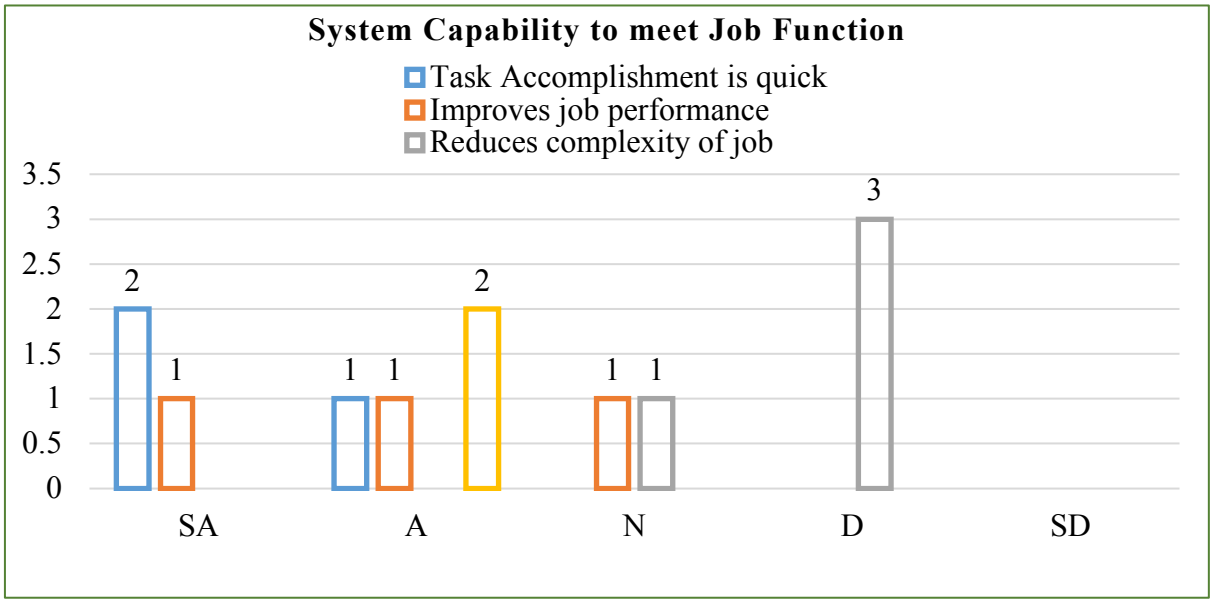


Figure 4.18. Civil Registration System – System Capability

4.4.2.10 System Portability

Given that the Civil Registration system can only run if Python, OpenCV's Boost Cascade and Xampp control which are open source programs are installed; the research validation participants were asked to determine if the system was portable enough. Figure 4.19 gives the responses to this question. As can be seen, 67% of the participants stated that the system was portable enough while 33% could not respond to the question and none of the participants stated that the system was not portable.

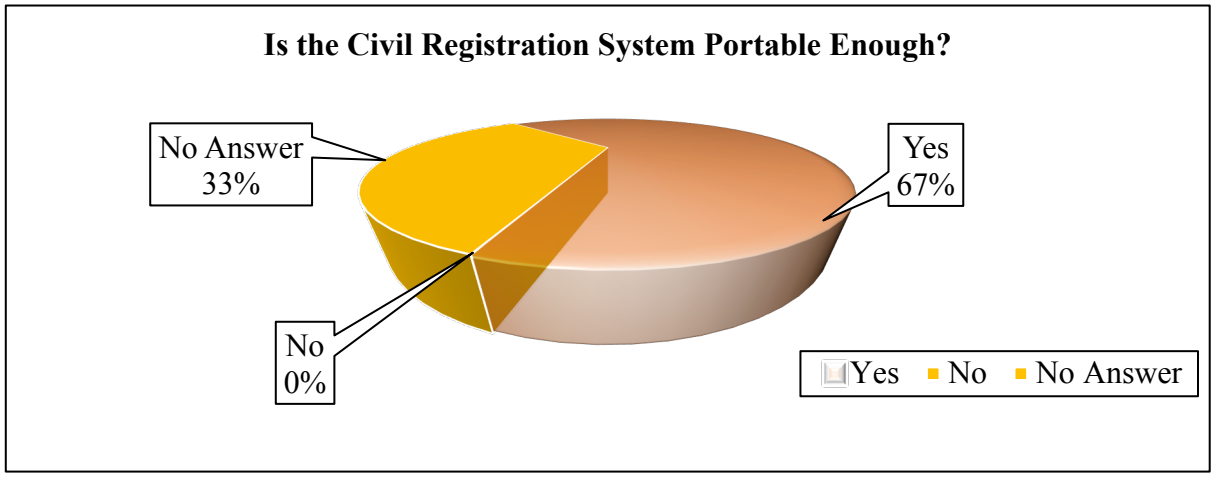


Figure 4.19. Civil Registration System – System portability

4.4.2.11 System Resources

Given that the civil Registration system requires systems resources of a computer with at least 4GB RAM, Hard disk capacity of at least 500GB and a web camera with a resolution of at least 0.9MP 16:9 (1280 x 720); the system validation research participants were asked to state whether these resources are too ambitious. Figure 4.20 shows the responses and as can be seen 3 participants stated that the resources were not too ambitious, 2 participants could not respond to the question and 1 participant was not sure.

Figure 4.20. Civil Registration System – System Resources

4.5. Recommendations

This section outlines the recommendations that have been collected from the research participants on what they believe should be present in the system to make the system more ideal and operate in such a way that it would meet the needs of MoHA and the civil registration officers who would be tasked with operating it on a daily basis.

4.5.1 Program Elements that must be removed

Table 4.4 shows the various inputs elements that must be removed from the Civil Registration system as far as the validation research participants were concerned. Participants stated that the middle name must NOT be set to a mandatory input field and this option must be removed from the system.

Table 4.4: Elements that must be removed from Civil Registration System

Element	Input For	Input Against or other	Percentage score to support decision
Middle Name	4 out of 6 participants say so	2 out 6 participants could NOT comment	67

4.5.2 Program Elements that must be added

Table 4.5 shows program elements that must be added to the civil registration system in order to make the system operate more optimally as far as the participants are concerned.

Table 4.5: Elements that must be added to the Civil Registration System

Element	Input For	Input Against or other	Percentage score to support decision
Module to print database listing	4 out of 6 participants say so	2 out 6 participants could NOT comment	67
Module to capture multi-mode biometric, say retina with face.	4 out of 6 participants say so	2 out 6 participants could NOT comment	67

4.6 Civil Registration System Prototype Screen Shots

4.6.1 Introduction

This section presents the results of the screen shots from the civil registration prototype. The results shown here are in sequenced form to depict a login and a full transaction to delivery of a civil document such as a Birth Certificate or NRC. Training is expected to be done at software deployment stage to ensure a correct login sequence. Figures 3.20 – 3.24 illustrate the login sequence; the remainder of the explanation covers operations after that login is successful with valid user credentials.

4.6.2 System Steps

To capture a civil record, a user must first click on the 'Birth Record' menu option which in turn loads the screen shown in Figure 4.21. In this screen a user is prompted to capture a face first before proceeding. To capture a face, click on the capture face button as shown in Figure 4.22. This button is located at the bottom section of the Facial Capture Screen.

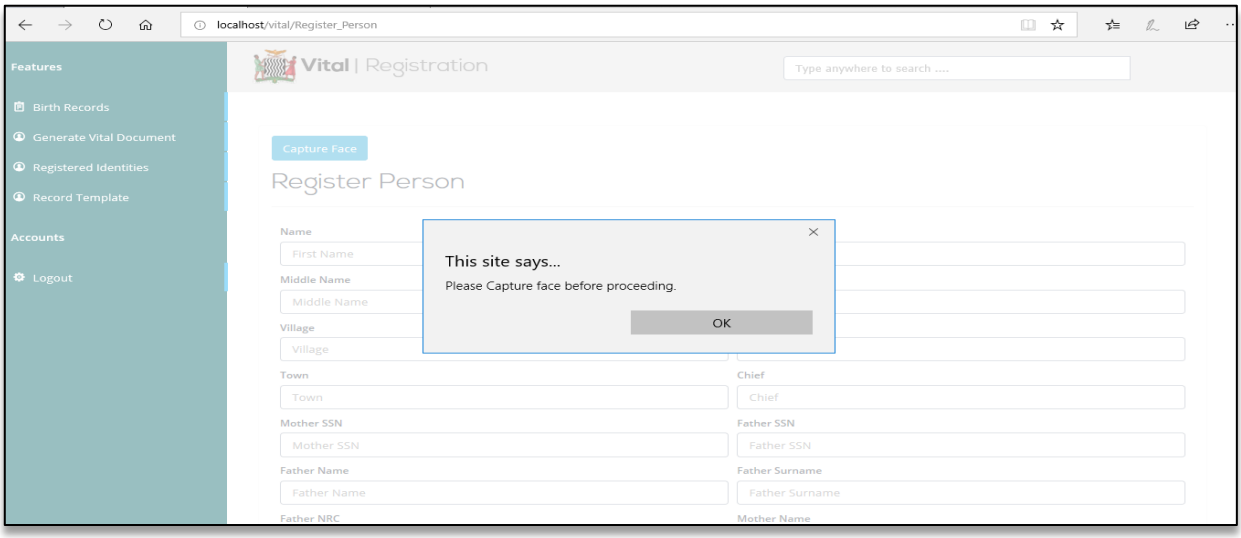


Figure 4.21. Main Screen – Prompt to Capture Face First

In Figure 4.21 the prompt or alert will be focused while the background is in watermark form. This allows the prompt to receive attention from the user of the system.

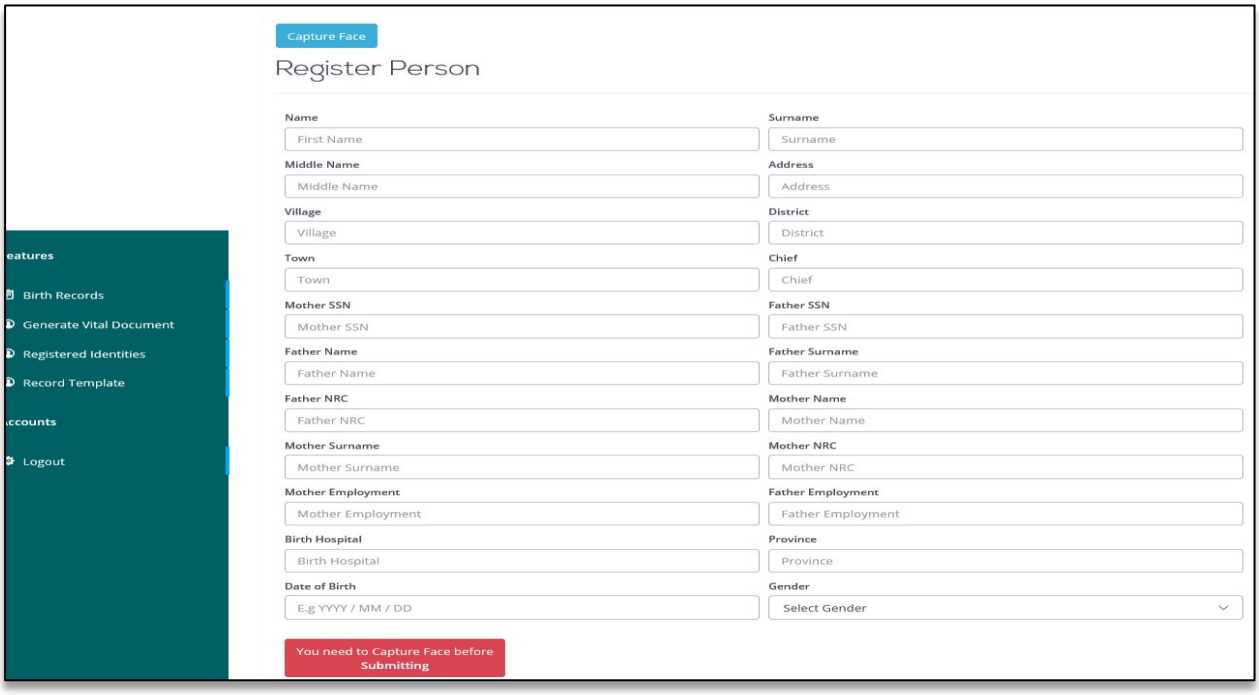


Figure 4.22. Main Screen – Process 2 Invoke Facial Capture Button

A Face Capture screen loads as shown in Figure 4.23. Once a biometric facial capture is made, a screen as shown in Figure 4.24 runs to allow for the input of personal details. A successful entry of details will then follow. Once complete, click on the submit button to commit the information collected to the MySQL Database. A citizen being captured must remain in a fixed position while this exercise progress. A processing time of approximately 5 – 10 seconds is required depending on lighting conditions and background objects. It is advised that a white background is used.

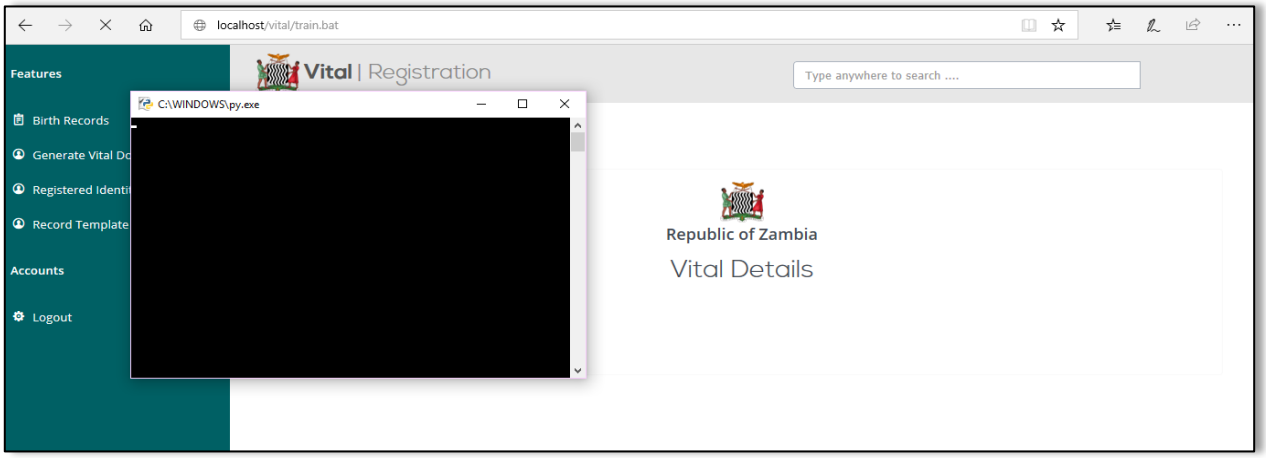


Figure 4.23. Facial Capture Screen

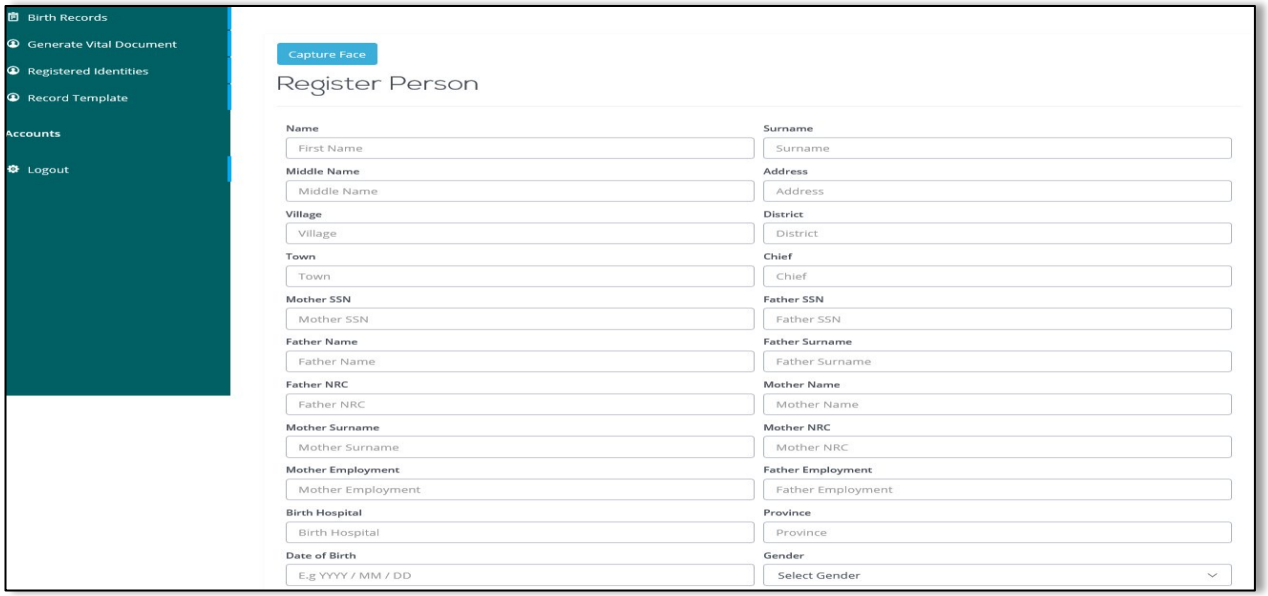


Figure 4.24. Citizen Data Capture

Once successfully committed, a prompt of this success is given and program control is passed to the system's desktop screen as shown in Figure 4.25 which will now show two options; calibrate and recognize face. A development of the strong classifier needed for facial recognition will need to be performed first before anything else. To do this click on the calibrate button. A calibration is run as shown in Figure 4.26.

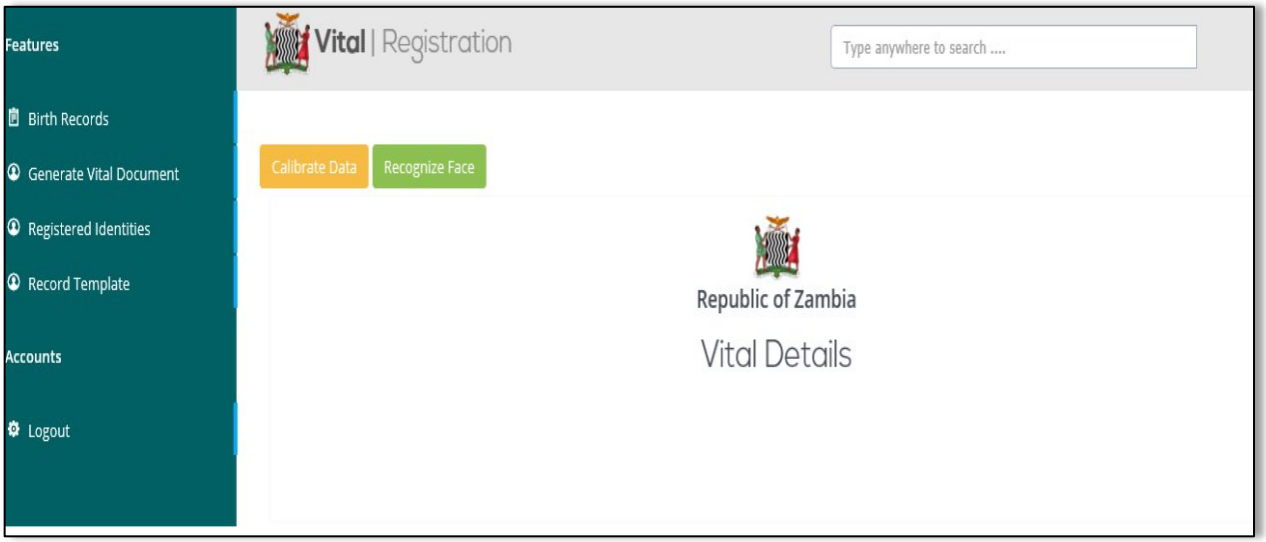


Figure 4.25. System Desktop

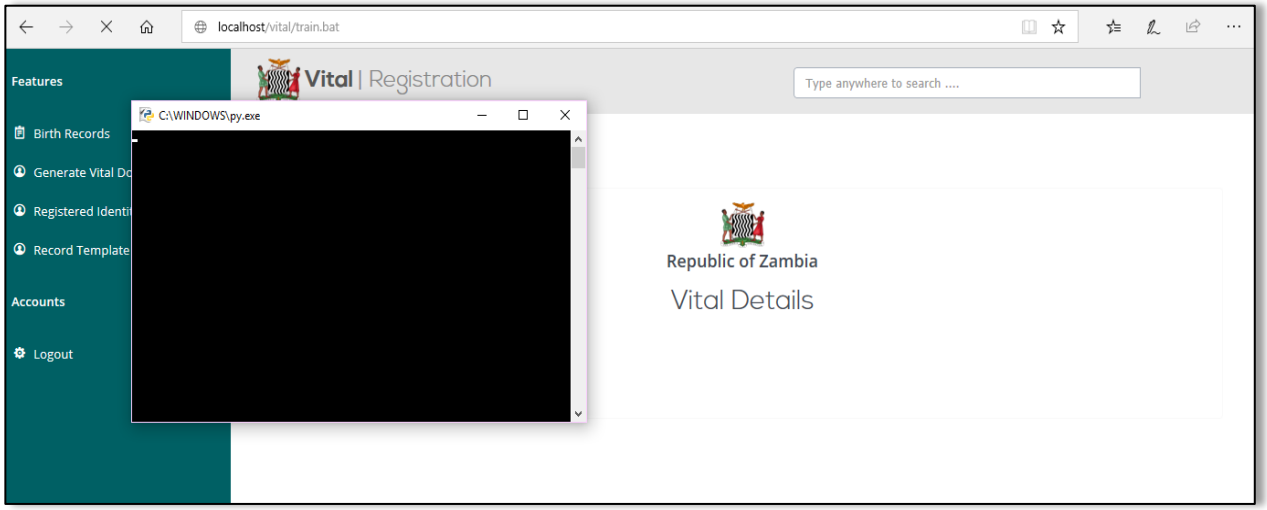


Figure 4.26. Calibration Screen

After calibration (or training), the program control returns to either Figure 3.23 or Figure 3.24 depending on the mode of access used.

A trial recognition must be made to ensure correct subject enrolment has been made. Click on the option 'Generate Vital Document" to invoke the frontal facial biometric module which will run and attempt to recognize the subject. A successful recognition results into a screen as shown in Figure 4.27.

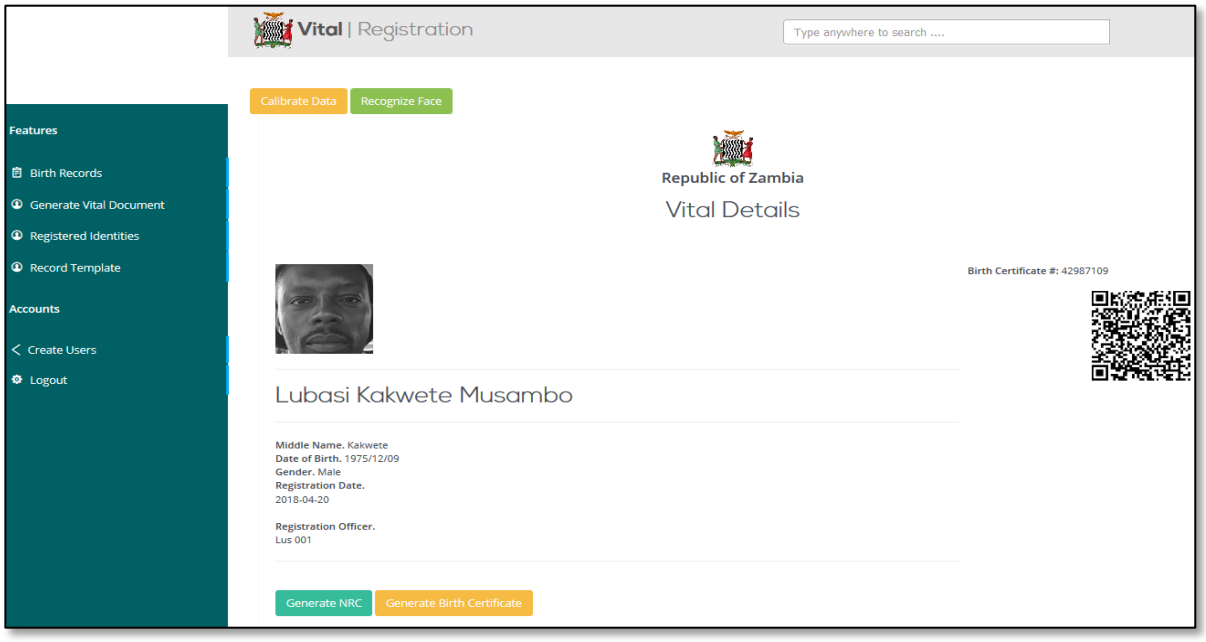


Figure 4.27. Temporal screen. Vital Document Generator

Request for a birth certificate by clicking on the "Generate Birth Certificate" button or request for a National Registration Card by clicking on "Generate NRC". A request for a birth certificate yields a screen as shown in Figure 4.28 and a request for a NRC yields a screen as shown in Figure 4.29.

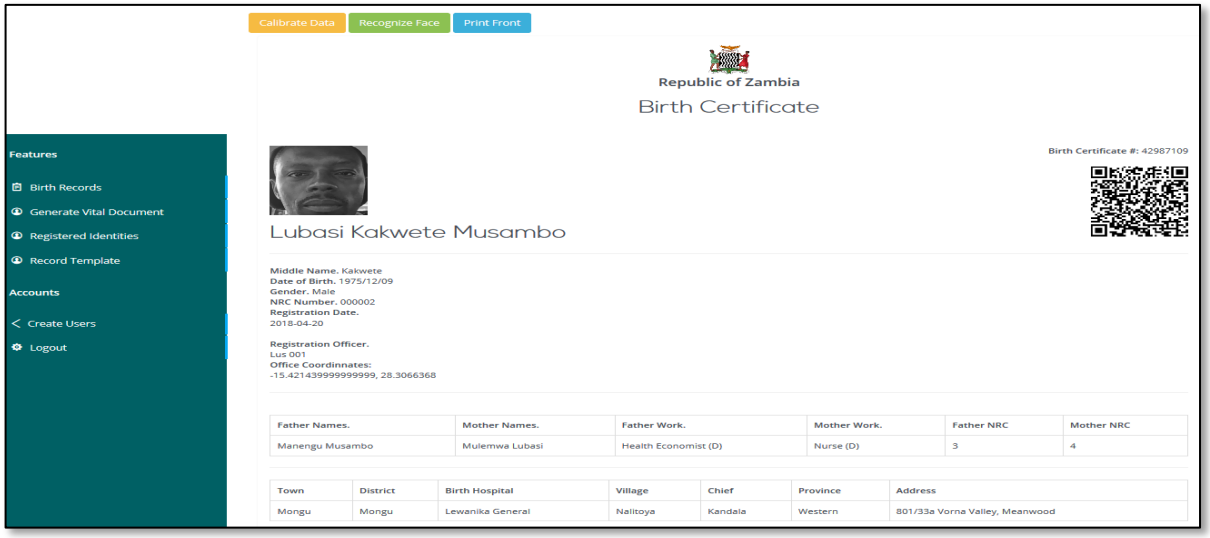


Figure 4.28. Proposed Birth Certificate

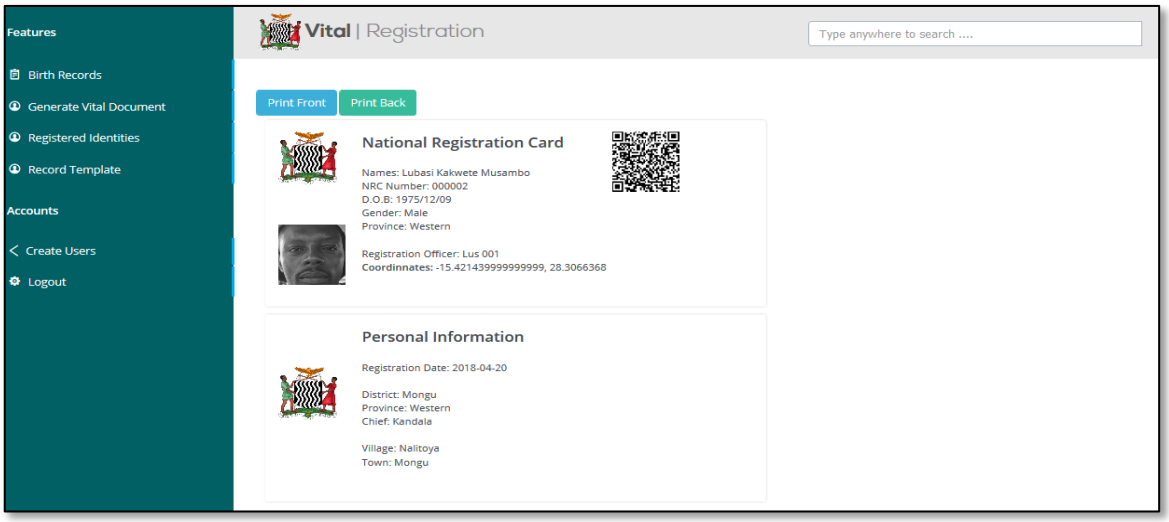


Figure 4.29. Proposed NRC

Notice that a QR Code as shown in Figure 4.30 is equally produced. The QR Code has birth certificate number, sex and registration date embedded for document marriage purposes and non-repudiation binding. A hardcopy printout of both documents is possible with NRCs printout optimized to ID paper size. Appropriate hardware with ID card print to PVC is recommended.

Figure 4.30. QR Code

For rural records, a click on the menu option “Record Template” will result into a screen as displayed in Figure 4.31. This template has been provided for because as shown in Figures 3.2a and 3.2b, no standard form exists for the capture of birth event details. This problem is exacerbated in rural areas where as shown in Figure 3.1 utilize village records to collect birth event details. These details are then transferred to an under-five card which again as shown in Figures 3.3a and 3.3b do not have a standard format. The birth template is made part of the

software model to ensure consistency of records and ensure a single method of data collection is achieved.

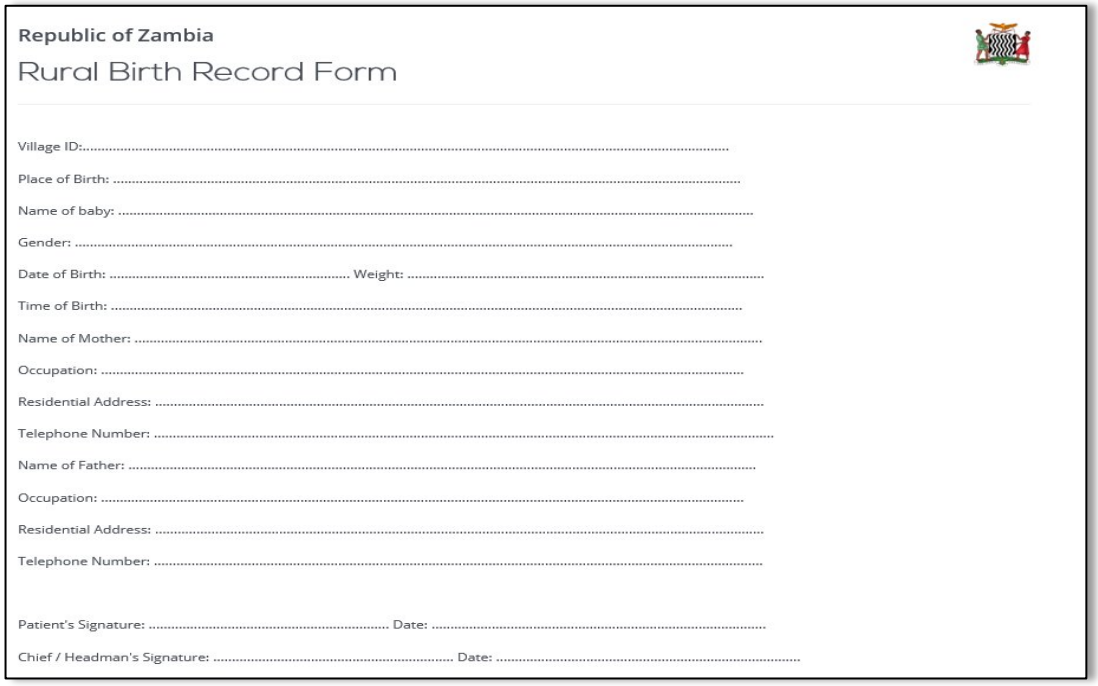


Figure 4.31. Proposed Birth Template

It is possible to view all registered identities within the system. This is made possible by clicking on "Registered Identities". Figure 4.32 illustrates the registered identities.

Further operations are possible from the system desktop or main menu screen (Figure 3.23 or 3.24) screen like record deletion. Clicking "Log out" button exits the program and returns control to the login screen (Figure 3.21).

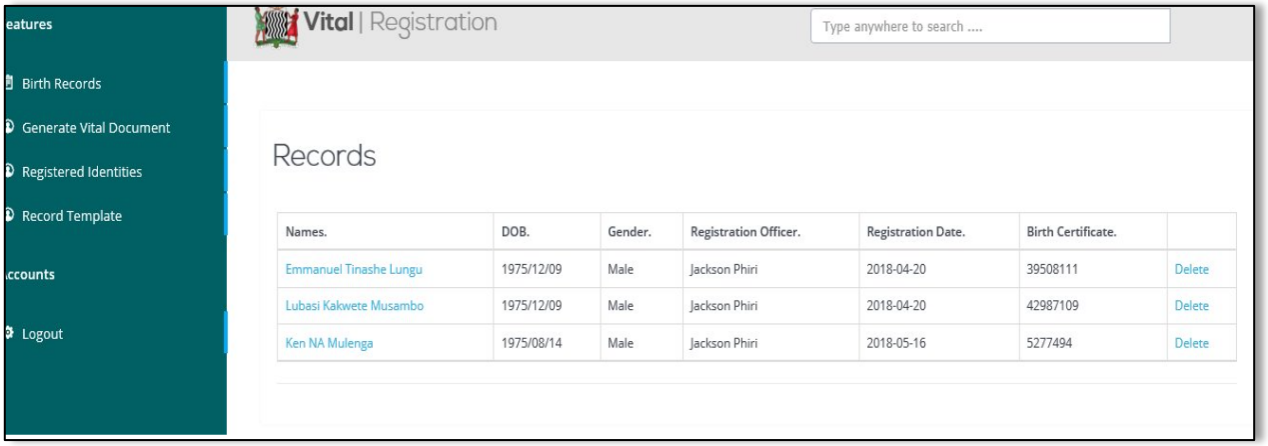


Figure 4.32. Registered Identities

During operations a user will come across prompts that are displayed as shown in Figure 4.33. These prompts are batch calls that are invoked by the system to Python. The facial biometric capture, identifier and recognizer are developed in Python and run using the OpenCV open source algorithm to perform the biometric operation. The web based module of the application is developed in pHp, HTML, JavaScript and MySQL. For the pHp to invoke the Python biometric module a batch call is made.

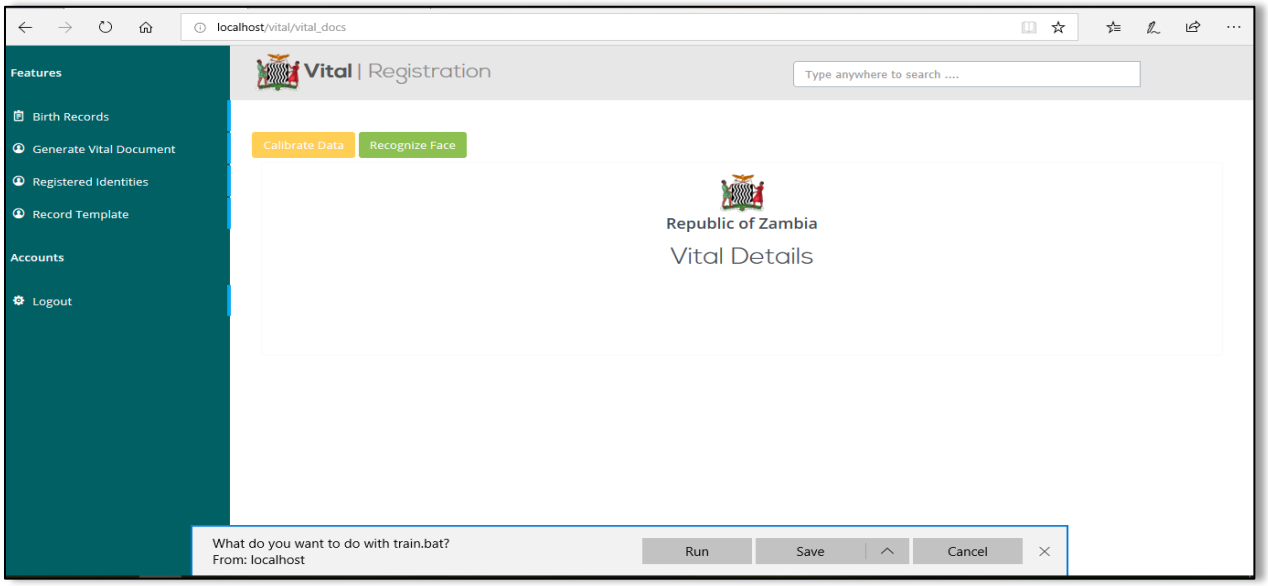


Figure 4.33. Batch Call

4.6.3 Biometric Storage Framework and Proposed Business Processes

In Figure 3.9 the author proposes an automated version of the civil registration processes that is suitable for the Zambian environment. The proposed mechanism will utilize a suitable biometric model that can capture an individual's biometric facial features and use those features to perform an authentication in order to award either a birth certificate or a NRC. To increase the security of the biometric model an information fusion technique as proposed by Phiri et. al [97] can be developed.

A user creation screen is added to the appendix to show how a new system user can be created on the system.

An automated version of the civil registration process eliminates the need to have a third party authentication via general Affidavit Form N (Figure 3.4). This increases the security of the civil data as integrity is maintained. We further propose that a centralized civil database be

created to house all civil data. The advantages of this centralized database will be equivalent to Singh et. al [157] and Chiffelle et. al [158].

Working closely with the Zambia Bureau of Standards (ZABS), ZICTA ought to develop and enforce a guidance on how to manage biometric data in Zambia. The biometric data is taken to mean a biometric reference which is a distinctive, measurable datum that can be used to label or describe an individual. The ISO 24745 does not describe physical security aspects of cryptographic systems though it can be used to guide biometric data storage in Zambia. This gap must be born into the design of any framework for biometric data. This framework can be understood to be a basic assembly that can support the use, storage and maintenance of the biometric data in Zambia. The ISO 24745 specifies issues to do with:

(a) An investigation, study and understanding of the threats to and mitigations that are present in a biometric and biometric system application or module, this includes models of such applications [112].
(b) A definition of the sound security requirements for ensuring a secure bind between a biometric locus (point of reference) and an identity reference (or entity) [112].
(c) Specifications for biometric system application models with different developments for the storage and comparison of biometric references [112].
(d) A thorough regulation on the provision of protection for an individual's privacy during the processing or any form of biometric information of that individual [112].

ISO 24745 pledges hindrance to biometric data theft or an unauthorized access by satisfying irreversible transform of operations at data storage. This guarantees that biometric data is not available for any other use apart from its' intended purpose. Irreversible transforms such as asymmetric cryptography must be applied to biometric data at storage time. ISO 24745 also pledges unlink-ability of stored biometric references. Biometric data cannot be linked across applications, systems, modules or databases. ISO 24745 finally pledges confidentiality to protect biometric references against access by any unauthorized entity. The occurrence of this threat would result into privacy risk issues. Cryptographic engineering must applied here as a contraceptive to protect or conceal biometric data.

Because Zambia has no biometric standard or law to supervise biometric data, a suitable biometric framework based on the ISO 24745 can be developed along the following options:

i. Storage of a biometric reference on a server and allow the server to compare input against reference. In this arrangement the server performs all the work and based on its findings, it may allow or deny access or authentication.

ii. Storage of biometric reference on a hardware security module (token) and then allow the server to compare the biometric reference which it can use to allow or authenticate an entity.

iii. Storage of biometric reference on a computer server and compare that reference on a user client computer.

The above options can be rearranged in such a way that the user client computer system takes the role of the server. A final option would be to store the reference on a cloud storage system and allow either the user client computer to compare or the cloud mechanism to compare the reference.

The author holds the belief that the advantages advanced by Mutale and Phiri [159], Vincent et al. [158], Singh and Malhotra [157] and King [160] on a central storage system are sufficient to advance the logic of a central storage framework of biometric data.

Considering all, we recommend the following biometric framework setup as shown in Figure 4.34.

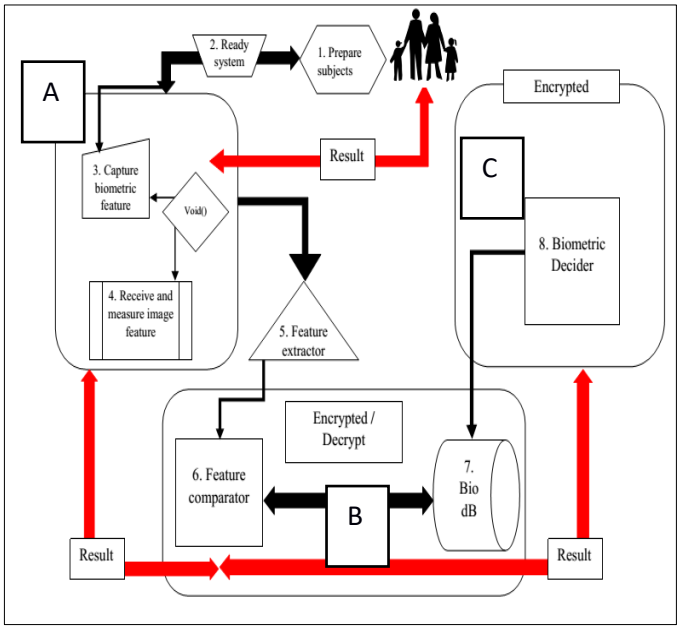


Figure 4.34. Proposed Zambian Biometric Framework. Adapted from [111]

Where:

A = user point biometric collection center (biometric data users)

B = ZICTA biometric central repository center

C = ZICTA biometric analyzer

A can be any user point, regulated and accredited by ZICTA;

B and C are at ZICTA and are a strict access controlled center.

4.7 Conclusion

In the chapter we have presented various results that were collected during the baseline study of the research. The collected information was analysed using Microsoft Excel which is an analysis software developed and maintained by Microsoft. We have presented the results using various tools such as bar charts, per charts and tables. We have also demonstrated the Civil Registration System software operations via screen shots of the same. In the last section we present what we consider to be an ideal biometric framework that can be adopted in the Republic of Zambia so that it can supervise the use of biometric data.

CHAPTER 5

DISCUSSION AND CONCLUSION

5.1 Introduction

In this chapter, we discuss the results presented in Chapter 4. The information collected in the baseline study of the research and presented in the Chapter 4 are discussed here. We focus on discussing the results by referring the findings to the research study objectives 1 and 2. This chapter also includes the conclusion, and recommendations of the study. The chapter closes by highlighting possible future works.

5.1.1 Baseline Study

Chapter 51 of the laws of Zambia, the Birth and Death Registration Act supervises the civil registration processes in the Republic of Zambia. The civil registration process is centralised and mostly manual. Two ways of performing civil registration exist in Zambia; The Urban route and the Rural route. The entire civil registration process is centralised and is performed by the Civil Registrar's office at the Ministry of Home Affairs. The registration process initiates at a place of birth (health facility) for urban situations and village secretary for rural situations. For the rural birth, the village birth registration details are transported into an under-five card clinic card at any nearest health centre. From here, the birth details can then be transported to civil registration centres via the parents / guardian. In either case of birth, the details must be authenticated by General Form Affidavit N when applying for a civil document such as a birth certificate or NRC. The current civil registration is manual-based with no form of computerisation. The entire process because of its' manual tasks results into inefficiency and inaccuracy plus duplication of inaccurate civil documents. The reliance on Affidavit Form N for information authentication generates various problems as far as information security is concerned. Some of the problems the use of General Affidavit Form N creates in the civil registration processes are poor authentication of the given personal details, non-repudiation challenges, costly service, poor service delivery by GRZ and redundancy of work and documents. To overcome these authentication problems and to enhance the civil registration process, a Civil Registration system was proposed incorporating Biometrics, Encryption, Geospatial data and QR Bar Codes.

Since the model is based on biometrics, a baseline study was carried out to collect data from the general public, government entities, commercial banks, students, ICT regulators and schools on their understanding, use and acceptance of biometrics as an authentication and civil registration tool suitable for a country such as the Republic of Zambia.

The findings from the baseline study are discussed in the following sections with references to Figures and Tables in Chapter four.

5.1.2 Awareness on Systems Security and Authentication

Figures 4.3 indicates that research participants' main source of knowledge on biometrics, biometric systems and information relating to this facet of ICT security is the Internet; 44 participants (the highest) reported this against 20 for TV as a source, 13 for access through friends while the other 20 and 3 reported through other means such as stories and radio respectively. Because of the nature of the Internet, it is possible that certain individuals may not acquire correct information that they may apply accurately in far as biometrics and biometric systems are concerned. Implementing a biometric system is practical in nature and to acquire information only by written texts via the Internet may not give an individual accurate and reliable information on the area of biometrics and information security aspects that relate directly to biometric and biometric systems.

Figure 4.6 shows that out of 100 participants, 20% stated that biometric data is ideal for criminal management purposes i.e. suspect identification systems and others related while 20% report that biometrics are ideal for information security services and 12% report that biometrics are ideal for Government services, 19% report that biometrics are ideal for medical purposes and lastly 3% report that biometrics can be ideal for other uses such as commercial applications like vehicular start. This agrees with Prabhakar et al. [161] and Musambo et al. [107] who equally report that biometrics can be ideal for such purposes.

Figure 4.8 and Table 4.1 indicate that participants reported that they support biometric data usage based on various reasons such as their perception they hold toward the biometric system. This finding agrees with Onywoki et. al [140] who argues that perception plays a role on acceptance of a biometric system. Figure 4.9, 4.10 and Table 4.3 which report that participant's desire to have a ZICTA Biometric storage agree with Mutale et. al [159] in their

argument to have a central archiving system for records. This central storage can be a biometric data system for the entire country of Zambia.

5.1.3 Biometric Standard and Biometric Framework

Figure 4.4 indicates that 26% of the research participants reported to have a biometric framework installed in their organisation that supervises the usage of those organisations biometric data while 66% reported that no such biometric framework exists in their organisations and 8% could not respond to this question. From this information, the 26% who responded as having a biometric framework could not state what that biometric framework is as it would appear they do not know what a biometric framework must do to supervise the organisation's biometric data. This illustrates that the need for knowledge and awareness in the area of biometrics is key as it appears that organisations that collect biometric data do not educate the owners of the biometric data on how and where their data is managed from. This also agrees with figure 4.5 where individuals do not seem to understand where their biometric data must be kept as 16% of the participants report that the Internet must house such data while 50% report that their work places must retain such data and 34% give wide answers such as government agencies must keep such information. This calls for a centralised location of such data.

Figure 4.7 reports that 98 of the research participants are not aware of any biometric innovation such as a framework that the government of Zambia is implementing while 1 reports that such an innovation is in place. This information finding can be made to argue a case that since in figure 4.5 individuals are not certain as to where biometric data can stored then there is a lack of know-how and information dissemination on biometrics in Zambia.

Table 4.1 and Figure 4.9 report that participants desire Zambia to have a biometric framework developed that can supervise the usage of biometrics and biometric data. Figure 4.10 reports that participants would support storage of their biometric by a biometric framework running through a standard. This further indicates and agrees with the ECTA 2009 [129] and the Zambian ICT policy [130] which does NOT specify a framework or standard to supervise biometrics in Zambia in the sense that the current law requires change or amendment.

5.2 Conclusion

The aim of the study was to develop a software model that automates the civil registration by capturing birth details of an individual through biometrics and producing a civil document such as birth certificate and NRC by incorporating biometrics, QR Bar Codes, Encryption and Geospatial data. The software model once fully developed, it is hoped can lessen the major challenges in the existing civil registration processes in the Republic of Zambia. Currently Zambia has NO automated civil registration system, NO standard or frameworks on biometrics. As such, the current challenge of a lack of an automated civil registration system in the current business processes of civil registration was used to develop a web-based civil registration application in order to mitigate the identified drawbacks. The objectives of the study were to develop a model after identifying the challenges in the current business processes. These objectives have been met as the software model has been developed to automate the civil registration system. Further the objectives were such that ISO standards were to be used to ensure the model developed fits into the ISO regulations; to be specific ISO 24745 and ISO 27001 standards. These objectives have equally been met as a biometric framework has been proposed to supervise the biometric data usage in the Republic of Zambia. Based on the objectives for the study, the following conclusions were arrived at; various forms of biometrics can be used in authentication systems; The general security challenges of information security in civil registration systems in developing countries can be overcome by the integration of biometrics features in the authentication systems and a cheaper solution for most developing countries is the use of open source tools and cheaper devices. Our study was proposing the use of OpenCV for Biometric Facial recognition and simple cheaper Web Camera such as one that comes integrated in most mobile computing devices. The software model achieves ≈ 67% acceptance rate and a false acceptance rate of 33%.

This study does not discuss the limitations inherent in the use of geospatial data especially for regions such as Zambia nor does it provide a basis for evaluating such data. This study, equally is limited to issues that relate to the development of the Zambian Information and Communication Technology Policy and development of a biometric law for Zambia.

5.3 Recommendations

The following are the recommendations to improve the existing civil registration system in Zambia:

a) Development of a multi-mode biometric authentication tool biased towards black people detection that is integrated into a health facility;
b) Generation of a central database that interlinks health-centers, education centers and NGO centers, private sector Organisation to enable authentication and reduce on redundancy of documents;
c) Non-government bodies (banks etc.) must not collect or retain biometric data. Only MoHA must be tasked with this facility in such a way that MoHA can control access to citizen biometric data and as a way to allow access and limit abuse charge a fee to all non-government institutions that would want use of this data;
d) The Government of Zambia through the Ministry of Home Affairs and The Ministry of Communications must develop a policy and legal framework that can supervise the use of biometrics in Zambia;
e) Following in on (d) above the Ministry of Communications working with other government units such as ZICTA, ZABS, Smart Zambia and CCPC can develop an interlinked Smart hub for citizen biometric data that can help Zambia meet its dream of becoming a smart country.

5.4 Future Works

For future works, the following are recommended:

i. a large dataset testing compromising of a majority of black people for a full proof authentication system based on facial biometrics;
ii. a study on the development of a Zambian Biometric Policy and National Law;

REFERENCES

1 Constitution, "The Births And Deaths Registration Act 1973," In *The Constitution Of Zambia*, Lusaka, Ministry Of Home Affairs, 2016, Pp. 1-43.

2 K. Kambole And E. M. Silanda, "The Current Status Of Civil Registration In Zambia," Addis Ababa, 1994.

3 Un, "Status Of Civil Registration And Vital Statistics In The Sadc Region," United Nations, Lusaka, 2010.

4 Lcc, "Birth Registration," 2017. [Online]. Available: Www.Lcc.Gov.Zm/Birth-Registration. [Accessed 8 February 2017].

5 Registrationact, "The Registration Act Of 1973 And 1994," *Constituition,* Pp. 1-43, 23 March 1973.

6 Moha, "Improvement Of Civil Registration And Vital Statistics In Sadc Region," *Workshop On The Improvement Of Civil Registration And Vital Statistics In Sadc Region,* Pp. 1-23, 2016.

7 F. S. Gethsemane Mwizabi, "Birth Certificate Mystery: Zambia Should Decentralise Registration," *Times Of Zambia,* 20 June 2014.

8 Undesa, "Status Of Civil Registration And Vital Statistics In The Sadc Region," United Nations Department Of Economic And Social Affairs Statistics Division, Switzerland, 2010.

9 S. Vaithyasubramanian, A. Christy And D. Saravanan, "Two Factor Authentications For Secured Login In Support Of Effective Information Preservation And Network Security," *Arpn Journal Of Engineering And Applied Sciences,* Vol. 10, No. 5, Pp. 1-4, 2015.

10 H. Lumba, "Plug Loopholes In Nrc Issuance," *Times Of Zambia,* Pp. 1-15, 2015.

11 J. Konayuma, "Share D Nrc Numbers: Buck Stops At National Registration Department," *Zambia Daily Mail,* Pp. 1-15, 2015.

12 R. S. D. D. Efraim Turban, Decision Support And Business Intelligence Systems, Boston: Pearson, 2011.

13 L. Times, "National Registration Card Office In Ndola Burnt To Ashes," 2017. [Online]. Available: Www.Lusakatimes.Com/2017/12/26/National-Card-Office-Ndola-Burns-Ashes/. [Accessed 26 December 2017].

14 S. Taylor, "Tenth Symposium & Exhibition On Machine Readable Travel Documents (Mrtds) & Border Security," 7-9 October 2014. [Online]. Available: Https://Www.Icao.Int/Meetings/Mrtd-Symposium-2014/Documents/8_Pm_Taylor.Pdf. [Accessed 2 August 2018].

15 Constituion, "The Births And Deaths Registration Act 1973," In *The Constitution Of Zambia*, Lusaka, Ministry Of Home Affairs, 2016, Pp. 1-43.

16 Ine, "Vital Statistics Methodology," National Statistics Institute, Madrid, 2013.

17 S. Patel, "Why Civil Registration Matters In The Countdown To The Millennium Development Goals," The World Bank. Ibrd. Ida, 4 April 2011. [Online]. Available: Http://Blogs.Worldbank.Org/Developmenttalk/Why-Civil-Registration-Matters-In-The-Countdown-To-The-Millennium-Development-Goals. [Accessed 17 August 2018].

18 G. S. Service, "Civil Registration And Vital Statistics System In Ghana: Report On The Comprehensive Assessment," Ghana Statistical Service, Accra, 2015.

19 J. D. Poloko, "Bostwana Strategy For The Development Of Statistics (Bsds) Civil Registration And Vital Statistics (Cvrs) 2016 Progress Report," Ministry Of Nationality, Immigration And Gender Affairs, Gaberone, 17 March 2017.

20 Unicef, "Strengthening Birth Registration In Africa: Opportunities And Partnerships Technical Paper," Unicef, Switzerland, 2010.

21 Immihelp.Com, “Us Birth Certificate,” 2017. [Online]. Available: Http://Www.Immihelp.Com/Nri/Birthcertificate.Html. [Accessed 16 February 2017].

22 Crown, “Register A Birth,” 2017. [Online]. Available: Https://Www.Gov.Uk/Register-Birth. [Accessed 16 February 2017].

23 Migrationsverket, “Libya-Report-Nationality-Registration-And-Documents-Netherlands-19122014,” Migrationsverket, Belgium, 2014.

24 Un, “Principles And Recommendations For A Vital,” *Statistical Papers, Series M No. 19/Rev.3,* Vol. St/Esa/Stat/Ser.M/19/Rev.3, No. Rev.3, Pp. 1-238, 2014.

25 Microsoft, “Bing Eu Identity Card,” Microsoft, 3 August 2018. [Online]. Available: Https://Binged.It/2o8aue4. [Accessed 3 August 2018].

26 M. Edgeworth, “How To Get Eu Citizenship, Country By Country,” Billford, 2014 November 2014. [Online]. Available: Https://Www.Thebillfold.Com/2014/11/How-To-Get-Eu-Citizenship-Country-By-Country/. [Accessed 2018 August 4].

27 Mlha, “Integration Of Civil Registration And Vital Statistics: And Identity Management Systems:Botswana Success Story,” Department Of Civil And National Registration: Ministry Of Labour And Home Home Affairs, Gaberone, September 2015.

28 Mlha, “National Identity Card (Omang),” Botswana Government (Mlha), 2011. [Online]. Available: Http://Www.Gov.Bw/En/Ministries--Authorities/Ministries/Ministry-Of-Labour--Home-Affairs-Mlha/Tools--Services/Services--Forms/National-Identity-Application/. [Accessed 3 August 2018].

29 Gsma, “Birth Registration In Tanzania:Tigo’s Support Of The New Mobile Birth Registration System,” Gsma Head Office, London, 2016.

30 A. Mtulya, “Tanzania: Unicef Moves To Reduce Birth Certificate Burden,” The Citizen, 17 September 2016. [Online]. Available: Https://Allafrica.Com/Stories/201609190299.Html. [Accessed 3 August 2018].

31 G. O. Tanzania, “One Day Stakeholders Consultative Meeting On The Civil Registration And Vital Statistics (Cvrs),” Government Of Tanzania, Dar Es Salaam, 22 September 2015.

32 K. Makoye, “Tanzania Launches New Id Cards To Combat Election Fraud,” Thomson Reuters Foundation , 27 February 2013. [Online]. Available: Http://News.Trust.Org/Item/20130227092500-Jm6av/. [Accessed 3 August 2018].

33 P.S Ankrah, “Birth Registration In Ghana,” The Birth Registration Workshop For Anglophone Countries In Africa, Kampala, Uganda, 2002.

34 Editor, “Ghana Launches New National Id Card,” Modern Ghana, 15 September 2017. [Online]. Available: Https://Www.Modernghana.Com/News/802968/Ghana-Launches-New-National-Id-Card.Html. [Accessed 3 August 2018].

35 K. Kambole And E. M. Silanda, “The Current Status Of Civil Registration In Zambia,” Addis Ababa, 1994.

36 Phoenixfmzambia, “Most Zambians Not Registered By Ministry Of Home Affairs,” Phoenixfmzambia, 24 July 2018. [Online]. Available: Https://Web.Facebook.Com/Radiophoenixzambia/?Hc_Ref=Arqxayyxw2xg3sd3axytyixl0t5bmkms3lllsgwypoxlwhctgyuidqro-5h6tl-Iyqs&Fref=Nf. [Accessed 28 July 2018].

37 Moha, “National Strategic Action Plan For Reforming And Improving Civil Registration And Vital Statistics 2014-2019,” Moha, Grz, Lusaka, 2014.

38 N. Desk, “Most Zambians Not Registered By Ministry Of Home Affairs,” Zambian Eye, 24 July 2018. [Online]. Available: Https://Zambianeye.Com/Most-Zambians-Not-Registered-By-Ministry-Of-Home-Affairs/. [Accessed 28 July 2018].

39 Countryeconomy, “Zambia,” Countryeconomy, 28 July 2018. [Online]. Available: Https://Countryeconomy.Com/Demography/Population/Zambia. [Accessed 28 July 2018].

40 Who, “Civil Registration: Why Counting Births And Deaths Is Important,” Who, 30 May 2014. [Online]. Available: Http://Www.Who.Int/En/News-Room/Fact-Sheets/Detail/Civil-Registration-Why-Counting-Births-And-Deaths-Is-Important. [Accessed 2 August 2018].

41 P. Works, “Advantages And Disadvantages Of Technologies,” Pb Works, 7 February 2018. [Online]. Available: Http://Biometrics.Pbworks.Com/W/Page/14811349/Advantages%20and%20disadvantages%20of%Technologies. [Accessed 7 February 2018].

42 Crown, “Police And Crimminal Evidence Act 1984,” Legislation, 15 July 2018. [Online]. Available: Www.Legislation.Gov.Uk/Ukpga/1984/60/Contents. [Accessed 15 July 2018].

43 J. R. Vacca, Computer And Information Security Handbook, Amsterdam: Mk, 2009.

44 Pcworld, “Why Convenience Is The Enemy Of Security,” Idg Communications Inc., 18 August 2018. [Online]. Available: Https://Www.Pcworld.Com/Article/257793/Why_Convenience_Is_The_Enemy_Of_Security.Html. [Accessed 18 August 20181].

45 N. Ferguson, B. Schneier And T. Kohno, Cryptography Engineering: Design Principles And Practical Applications, Indianapolis: Wiley, 2010.

46 K. Martin, Everyday Cryptography: Fundamental Principles & Applications, New York: Oxford University Press, 2012.

47 W. Stallings, Network Security Essentials, New York: Prentice Hall, 2011.

48 O. Nmap, “Nmap,” 7 May 2017. [Online]. Available: Https://Nmap.Org/.

49 D. Goodin, “Nsa-Leaking Shadow Brokers Just Dumped Its Most Damaging Release Yet,” Cnmn Collection, 14 May 2017. [Online]. Available: Https://Arstechnica.Com/Information-Technology/2017/04/Nsa-Leaking-Shadow-Brokers-Just-Dumped-Its-Most-Damaging-Release-Yet/. [Accessed 6 February 2018].

50 A. Zaharia, “What Is Ransomware – 15 Easy Steps To Protect Your System [Updated],” Heimdal Security, 15 May 2017. [Online]. Available: Https://Heimdalsecurity.Com/Blog/What-Is-Ransomware-Protection/. [Accessed 6 February 2018].

51 A. Thapa, “Social Engineering,” *Cissp,* Pp. 1-11.

52 J. M. Stewart, E. Tittel And M. Chapple, Certified Information System Security Professional, Canada: Wiley, 2008.

53 L. K. Musambo, M. Chinyemba And J. Phiri, “Identifying Botnets Intrusion & Prevention – A Review . Zambia Ict Journal, Dec. 2017. Available At: Http://Ictjournal.Icict.Org.Zm/Index.Php/Zictjournal/Article/View/28,” *Zambia Ict Journal,* Vol. 1, No. 1, Pp. 63-68, 2017.

54 D. Bader, “Samsung Galaxy S9 & S9+: Everything You Need To Know!,” Android Central, 25 February 2018. [Online]. Available: Https://Www.Androidcentral.Com/Samsung-Galaxy-S9. [Accessed 12 March 2018].

55 Cnet, “Hp Spectre X360 13 (Late 2017),” Cbs Interactive Inc, 9 February 2018. [Online]. Available: Https://Www.Cnet.Com/Products/Hp-Spectre-X360-13-Late-2017/. [Accessed 12 March 2018].

56 Instagram, “#Whp,” Instagram, 9 March 2018. [Online]. Available: Http://Blog.Instagram.Com/. [Accessed March 13 2018].

57 Facebook, “Facebook Principles,” Facebook, 2018. [Online]. Available: Https://Web.Facebook.Com/Principles.Php?_Rdc=1&_Rdr. [Accessed 12 March 2018].

58 M. Bergman, “The Deep Web: Surfacing Hidden Value,” In *Cs895 – Web-Based Information Retrieval*, Washington, 2011.

59 C. Cimpanu, “There Are Only 30,000 Websites On The Dark Web,” 2016. [Online]. Available: Http://News.Softpedia.Com/News/There-Are-Only-30-000-Websites-On-The-Dark-Web-502725.Shtml. [Accessed 29 April 2017].

60 P. Alto, “Top 10 Social Networking Threats,” Network World, 12 July 2010. [Online]. Available: Https://Www.Networkworld.Com/Article/2213704/Collaboration-Social/Top-10-Social-Networking-Threats.Html. [Accessed 12 March 2018].

61 S. Sehgal, “Road Towards Cloud Computing - What Are The Issues? Part 1,” 2016. [Online]. Available: Www.Simplilearn.Com/Cloud-Computing-Issues-Part-I-Article. [Accessed 30 January 2018].

62 U. Salesforce, “Why Move To The Cloud? 10 Benefits Of Cloud Computing,” Salesforce, 17 November 2015. [Online]. Available: Https://Www.Salesforce.Com/Uk/Blog/2015/11/Why-Move-To-The-Cloud-10-Benefits-Of-Cloud-Computing.Html. [Accessed 12 March 2018].

63 R. B. Thirumala And N. Vurukonda, “2nd International Conference On Intelligent Computing, Communication & Convergence,” Odisha, India, 2016.

64 M. Berry, “Network Security: Top 5 Fundamentals,” It Manager Daily, 18 August 2018. [Online]. Available: Http://Www.Itmanagerdaily.Com/Network-Security-Fundamentals/. [Accessed 18 August 2018].

65 W. Stallings, Cryptography And Network Security, Upper Saddle River: Prentice Hall, 2006.

66 S. Gatti, Project Finance In Theory And Practice, Burlington: Elsevier, 2008.

67 Isaca, “Insights And Resources For The Cybersecurity Professional,” 2009. [Online]. Available: Https://Www.Isaca.Org/Knowledge-Center/Research/Researchdeliverables/Pages/An-Introduction-To-The-Business-Model-For-Information-Security.A. [Accessed 17 March 2018].

68 K. Singh, “It Infrastructure Security-Step By Step,” *Infosec Reading Room,* Pp. 1-11, 2001.

69 Investopedia, “What Is An 'Industry',” Investopedia, Llc., 18 March 2018. [Online]. Available: Https://Www.Investopedia.Com/Terms/I/Industry.Asp. [Accessed 18 March 2018].

70 Investopedia, “Industry Handbook: Porter's 5 Forces Analysis,” Investopedia, 18 March 2018. [Online]. Available: Https://Www.Investopedia.Com/Features/Industryhandbook/Port. [Accessed 18 March 2018].

71 M. Korolov, “Banks Get Attacked Four Times More Than Other Industries,” Idg Communications, Inc., 23 June 2015. [Online]. Available: Https://Www.Csoonline.Com/Article/2938767/Advanced-Persistent-Threats/Report-Banks-Get-Attacked-Four-Times-More-Than-Other-Indust. [Accessed 18 March 201818].

72 A. Munns And R. Schmittling, “Performing A Security Risk Assessment ,” Isaca, 2018. [Online]. Available: Https://Www.Isaca.Org/Journal/Archives/2010/Volume-1/Pages/Performing-A-Security-Risk-Assessm. [Accessed 18 March 2018].

73 Tech-Faq, “Designing Network Infrastructure Security,” Independent Media, 17 August 2018. [Online]. Available: Http://Www.Tech-Faq.Com/Designing-Network-Infrastructure-Security.Html. [Accessed 18 August 2018].

74 J. C. A. D. Yeates, Project Management For Information Systems, Uk: Pearson Education Ltd Isbn: 978-0-13-206858-1 , 2008.

75 C. Bentley, Prince2™ Revealed, Colin Bentley (2010) Prince2™ Revealed, 2nd Edition Butterworth – Heinemann : Butterworth – Heinemann , 2010.

76 S. Dietrich And D. Dittrich, “P2p As Botnet Command And Control: A Deeper Insight,” In *3rd International Conference On Malicious And Unwanted Software*, 2008.

77 M. Jones, “The Ultimate Guide To The Deep Web,” 2014. [Online]. Available: Http://Www.Sickchirpse.Com/Deep-Web-Guide. [Accessed 29 April 2017].

78 Cyber Operations Research And Analysis,, “Darknet Terminology: Definitions Of The Darknet, The Dark Web, And The Deep Web,” 2016. [Online]. Available: Https://Coar.Risc.Anl.Gov/Coar-Attends-Department-Of-Homeland-Security-Hosted-Darknet-Summit/. [Accessed 29 April 2017].

79 M. Bishop, H. Conboy, H. Phan And Borislava, “Insider Threat Identification By Process Analysis,” *Ieee Security And Privacy Workshops,* Vol. Doi 10.1109/Spw.2014.40, No. Doi 10.1109/Spw.2014.40, Pp. 251-264, 2014.

80 C. Brodie, “The Importance Of Security Awareness Training,” 24th, 2018 April 2018. [Online]. Available: Https://Www.Sans.Org/Reading-Room/Whitepapers/Awareness/Importance-Security-Awareness-Training-33013. [Accessed 24 April 2018].

81 L. Musambo And M. Chinyemba, “Ieee – 2017 International Conference In Information And Communication Technologies (Icict),” Lusaka, 2017.

82 Webfinance, “Culture,” Webfinance Inc, 24 April 2018. [Online]. Available: Http://Www.Businessdictionary.Com/Definition/Culture.Html. [Accessed 24 April 2018].

83 M. N. Nawi And H. . H. J. Jazri, “Inculcating The Culture Of Ict Security,” *Oecd Guidlines For The Security Of Information Systems And Networks: Towards A Culture Of Security,* No. 81829, Pp. 1-4, 2002.

84 Techopedia, “Operating System Security (Os Security),” Techopedia Inc, 8 May 2018. [Online]. Available: Https://Www.Techopedia.Com/Definition/24774/Operating-System-Security-Os-Security. [Accessed 8 May 2018].

85 Espin, “Third-Party Software Security Independent Audit Services,” Espin, 8 May 2018. [Online]. Available: Https://Www.E-Spincorp.Com/2018/02/22/Third-Party-Software-Security-Independent-Audit-Services/. [Accessed 8 May 2018].

86 R. Pooley And B. Palmer, “What Is The Insider Threat?,” The Security Company, Cambridgeshire, 2013.

87 Microsoft, “Microsoft Security Updates,” Microsoft, 8 May 2018. [Online]. Available: Https://Technet.Microsoft.Com/En-Us/Security/Bulletins.Aspx. [Accessed 8 May 2018].

88 Microsoft, “Patching,” Microsoft, 8 May 2018. [Online]. Available: Https://Msdn.Microsoft.Com/En-Us/Library/Windows/Desktop/Aa370578(V=Vs.85).Aspx. [Accessed 8 May 2018].

89 P. Dhivya, S. Mohanagowri And N. Saravanaselvam, “An Improved Authentication Framework Using Steganography Along With Biometrics For Network Security,” *Journal Of Computer Science And Information Technology,* Vol. 2, No. 10, P. 30 – 35, October 2013.

90 N. S. Abouzakhar, *Introduction To Intrusion Detection,* Hartfield: University Of Hertfordshire, 2012.

91 J. Trader, “Iris Scanners And Recognition: A Biometric Identification Technique For Aiport Security Systems,” 2014. [Online]. Available: Www.m2sys.Com/Blog/Guests-Blog-Posts/Iris-Scanners-Recogition-Biometric-Identification-Technique-Airport-Security-Systems. [Accessed 23 November 2017].

92 Parliament, “Biometrics & Security,” The Parliamentary Office Of Science And Technology, 7 Millbank, London Sw1p, 2001.

93 T. P. Keenan, “Hidden Risks Of Biometric Identifiers And How To Avoid Them,” *Blackhat Usa - University Of Calgary,* Pp. 1-13, 2015.

94 C. Stearns, “Special Populations In Education: Definition & Examples,” Study.Com, 7 February 2018. [Online]. Available: Https://Study.Com/Academy/Lesson/Special-Populations-In-Education-Examples.Html. [Accessed 7 February 2018].

95 Nlm, “Special Populations,” Substance Abuse And Mental Health Services Administration (Us), Rockville (Md), 7 February 2018. [Online]. Available: Https://Www.Ncbi.Nlm.Nih.Gov/Books/Nbk64230/. [Accessed 7 February 2018].

96 Irititech, “Are Iris Biometrics Affected By Lasik Eye Correction (Or Any Other Corrective Surgery) Or By Disease?,” Iritech Inc, 7 February 2018. [Online]. Available: Http://Www.Iritech.Com/Content/Are-Iris-Biometrics-Affected-Lasik-Eye-Correction-Orany-Other-Corrective-Surgery-Or-Disease. [Accessed 7 February 2018].

97 J. Phiri, T.-J. Zhao, H. C. Zhu And J. Mbale, “Using Artificial Intelligence Techniques To Implement A Multifactor Authentication System,” *International Journal Of Computational Intelligence Systems,* Vol. 4, No. 4, Pp. 420-430, 2011.

98 T. Ramu And T. Arivoli, “A Framework Of Secure Biometric Based Online Exam Authentication: An Alternative To Traditional Exam,” *International Journal Of Scientific & Engineering Research,* Vol. 4, No. 11, Pp. 52-59, November 2013.

99 R. Saini And N. Rana, “Comparison Of Various Biometric Methods,” *International Journal Of Advances In Science And Technology,* Vol. Vol 2, No. I, Pp. 1-7, 2014.

100 K. P. Tripathi And B. Vidyapeeth, “A Comparative Study Of Biometric Technologies With Reference To Human Interface,” *International Journal Of Computer Applications,* Vol. 14, No. 5, Pp. 1-6, 2011.

101 F. Alonso-Fernandez, J. Fierrez And J. Ortega-Garcia, “Quality Measures In Biometric Systems,” In *Ieee*, 2011.

102 A. Lanitis, “Facial Biometric Templates And Aging:Problems And Challenges For Artificialproblems And Challenges For Artificial,” In *Aiai-2009 Workshops Proceedings*, 2014.

103 B. Esme And B. Sankur, “Effects Of Aging Over Facial Feature Analysis And Face Recognition,” *Bogaziçi Un. Electronics Eng. Dept.,* Pp. 1-4, 2010.

104 D. Yadav, R. Singh, M. Vatsa And . A. Noore, “Recognizing Age-Separated Face Images:Humans And Machines,” *Plos One,* Vol. 9, No. 12, Pp. 1-22, 2014.

105 M. Rose, “Biometrics,” 21 February 2017. [Online]. Available: Www.Searchsecurity.Techtarget.Com/Definition/Biometrics. [Accessed 21 February 2017].

106 R. Rezaei, . H. . Z. Nafchi And S. Morales, “Global Haar-Like Features:A New Extension Of Classic Haar Featuresfor Efficient Face Detection In Noisy Images,” *R. Klette, M. Rivera, And S. Satoh (Eds.),* Pp. 302-313, 2014.

107 L. K. Musambo And J. Phiri, “Student Facial Authentication Model Based On Opencv’s Object Detection Method And Qr Code For Zambian Higher Institutions Of Learning,” *(Ijacsa) International Journal Of Advanced Computer Science And Applications,* Vol. 9, No. 5, Pp. 88-94, 2018.

108 L. O'gorman, “Comparing Passwords, Tokens, And Biometrics For User Authentication,” *Proceedings Of The Ieee,* Vol. 91, No. 12, Pp. 2021-2040, December 2003.

109 R. Circus, “The Many Ways Your Face Changes During Pregnancy,” Rebel Circus, 3 May 2017. [Online]. Available: Http://Www.Rebelcircus.Com/Blog/Many-Ways-Face-Changes-Pregnancy/. [Accessed 12 February 2018].

110 T. Hall, “Internet Learning, Internet Voting: Using Ict In Estonia,” *Ipsa,* P. 31, 2012.

111 C. Busch, “Busch-Eab-Iso-24745-120713.Pdf,” 7 July 2012. [Online]. Available: Https://Christoph-Busch.De/Files/Busch-Eab-Iso-24745-120713.Pdf. [Accessed 18 April 2018].

112 Iso, “Information Technology -- Security Techniques -- Biometric Information Protection,” Iso/Iec, June 2011 . [Online]. Available: Https://Www.Iso.Org/Standard/52946.Html. [Accessed 18 April 2018].

113 T. Kohno, A. Stubblefield, S. D. Wallach And D. A. Rubin, “Analysis Of An Electronic Voting System,” *Ieee Symposium On Security And Privacy 2004,* P. 23, 2004.

114 N. Guntupalli, P. D. Raju And S. Cheekaty, “An Introduction To Different Types Of Visual Cryptography Schemes,” *International Journal Of Science And Advanced Technology,* Vol. 1, No. 7, Pp. 198-205, September 2011.

115 Tutorialspoint.Com, “Cryptography - Quick Guide,” [Online]. Available: Http://Www.Tutorialspoint.Com/Cryptography/Cryptography_Quick_Guide.Htm. [Accessed 18 August 2018].

116 L. Petersen And B. S. Dave, Computer Networks: A Systems Approach, San Francisco: Elsevier, 2007.

117 C. Microsoft, “Microsoft Encarta,” Usa, 2009.

118 F. Hao, R. Anderson And J. Daugman, “Combining Cryptography With Biometrics Effectively,” University Of Cambridge, Cambridge, Uk, 2005.

119 V. Dail, “Iris Recognition Vs. Biomettric Scanning - How Are They Different?,” 2017. [Online]. Available: Www.Biometrics-Security-Devices.Com/Biometric-Retina.Html. [Accessed 15 February 2017].

120 Y. Liu, “Identifying Legal Concerns In The Biometric Context,” *Journal Of International Commercial Law And Technology,* Vol. 3, No. 1, Pp. 45-54, 2008.

121 P. D. Hert, “Biometrics: Legal Issues And Implications: Background Paper For The Institute Of Prospective Technological Studies, Dg Jrc – Sevilla, European Commission,” European Communities, 2005.

122 A. Hern And D. Pegg, “Facebook Fined For Data Breaches In Cambridge Analytica Scandal,” The Guardian, 11 July 2018. [Online]. Available: Https://Www.Theguardian.Com/Technology/2018/Jul/11/Facebook-Fined-For-Data-Breaches-In-Cambridge-Analytica-Scandal. [Accessed 15 August 2018].

123 J. Bambauer And J. E. Rogers, “Biometric Privacy Laws: How A Little-Known Illinois Law Made Facebook Illegal,” In *Programs On Economics And Privacy*, Virginia, 2017.

124 V. Díaz, “Legal Challenges Of Biometric Immigration Control Systems,” *Esta Revista Forma Parte Del Acervo De La Biblioteca Jurídica Virtual Del Instituto De Investigaciones Jurídicas De La Unam,* Vol. Vii, No. 1, Pp. 3-30, 2014.

125 Crown, “Data Protection,” Crown, 15 July 2018. [Online]. Available: Www.Gov.Uk/Dataprotection. [Accessed 15 July 2018].

126 Liberty, “The Human Rights Act,” Liberty, 15 July 2018. [Online]. Available: Www.Libertyhumanrights.Org.Uk/Human-Rights/What-Are-Human-Rights/Human-Rights-Act. [Accessed 15 July 2018].

127 Legislation, “Crimminal Justice And Police Act 2001,” Thomsonreuters, 15 July 2018. [Online]. Available: Www.Uk.Practicallaw.Thomsonreuters.Com. [Accessed 15 July 2018].

128 Legislation, “Uk - Immigration And Asylum Act 1999,” European Council On Refugees And Exiles, 11 November 199. [Online]. Available: Www. [Accessed 15 July 2018].

129 Parliament, *The Electronic Communications Transactions Act,* Lusaka: Grz, 2009.

130 Moct, National Information And Communication Technology Policy, Lusaka: Grz, April 2006.

131 J. Mwenda, “Govt. Introduces Extra Charge On Whatsapp Internet Calls,” *News Diggers,* No. 241, P. 1, 2018.

132 Iso, “We're Iso: We Develop And Publish International Standards,” Iso, 3 August 2018. [Online]. Available: Https://Www.Iso.Org. [Accessed 3 August 2018].

133 Iec, “What We Do,” Iec, 2018. [Online]. Available: Www.Iec.Ch/About/Activites/?Ref=Menu. [Accessed 4 August 2018].

134 Itgovernance, “Iso 27001, The International Information Security Standard,” It Governance Ltd, 2018. [Online]. Available: Www.Itgovernance.Co.Uk/Iso27001. [Accessed 4 August 2018].

135 S. Singh, “Qr Code Analysis,” *International Journal Of Advanced Research In Computer Science And Software Engineering,* Vol. 6, No. 5, Pp. 89-92, May 2016.

136 A. Mehta, “Qr Code Recognition From Image,” *International Journal Of Advanced Research In Computer Science And Software Engineering,* Vol. 5, No. 12, Pp. 781-785, 2015.

137 S. Rupinder And R. Narinder, “Comparison Of Various Biometric Methods,” *International Journal Of Advances In Science And Technology,* Vol. Vol 2, No. I, Pp. 1-7, 2014.

138 P. Viola And M. Jones, “Rapid Object Detection Using A Boosted Cascade Of Simple Features,” In *Conference On Computer Vision And Pattern Recognition 2001*, Cambridge, 2001.

139 L. Rainer, K. Kuranov And V. Pisarevsky, “Empirical Analysis Of Detection Cascades Of Boosted Classifiers For Rapid Object Detection,” *Mrl Technical Report,* Pp. 1-7, 2002.

140 E. O. Benson Onywoki, “A Framework For The Adoption Of Biometric Atm Authentication In The Kenyan Banks,” *Journal,* Pp. 1-12, 2016.

141 P. Pandey And M. M. Pandey, Research Methodology: Tools And Techniques, Romania: Bridge Center, 2015.

142 S. Macdonald And N. Headlam, Research Methods Handbook, Manchester: Th Centre For Local Economic Strategies.

143 Microsoft, “Get A Better Picture Of Your Data,” Microsoft, 13 April 2018. [Online]. Available: Https://Products.Office.Com/En-Us/Excel. [Accessed 13 April 13].

144 I. Jacobson, M. Christerson, P. Jonson And G. Overgaard, Object-Oriented Software Engineering: A Use Case Driven Approach, Patparganj: Pearson Education, 2004.

145 D. Avison And G. Fitzgerald, Information Systems Development: Methodologies, Techniques & Tools, Maidenhead, Berkshire: Mcgraw-Hill Education, 2002.

146 S. Bennet, M. Steve And F. Ray, Object-Oriented Systems Analysis And Design: Using Uml, New Delhi: Tatamcgrawhill, 2007.

147 C. Sialubanje, K. Massar, D. H. Hamer And R. A. Ruite, “Reasons For Home Delivery And Use Of Traditional Birth Attendants In Rural Zambia: A Qualitative Study,” *Bmc Pregnancy And Childbirth,* Vol. 15, No. 216, Pp. 1-12, 2015.

148 Php, “Base64_Encode,” The Php Group, 21 July 2018. [Online]. Available: Http://Php.Net/Manual/En/Function.Base64-Encode.Php. [Accessed 21 July 2018].

149 Opensource, “Open Source Initiative,” Opensource Org., 29 January 2019. [Online]. Available: Https://Opensource.Org. [Accessed 29 January 2019].

150 R. Coronel, S. Morris And P. Rob, Database Systems: Design Implementation & Management, Boston: Boston, Ma : Course Technology, 2013.

151 A. Mohan , C. Papageorgiou And T. Poggio, “Example Based Object Detection.,” *Ieee Transactions On Pattern Analysis And Machine Intelligence,* Vol. 23, No. 4, Pp. 349-361, 2001.

152 R. Raja, “Face Detection Using Opencv & Python: Beginers Guide,” Superdatascience.Com, 8 July 2017. [Online]. Available: Www.Superdatascience.Com. [Accessed 1 April 2018].

153 S.-K. Pavani, D. D. Delgado And A. F. Frangi, “Haar - Like Features With Optimally Weighted Rectangles For Rapid Object Detection,” *Elsevier,* Vol. 43, No. 160-172, Pp. 160-172, 2010.

154 Smartdraw, “Uml Diagram,” Smartdraw, 22 July 2018. [Online]. Available: Https://Www.Smartdraw.Com/Uml-Diagram/. [Accessed 22 July 2018].

155 D. Miessler, “Obsecurity Is A Valid Security Layer,” Danielmiessler, 25 October 2017. [Online]. Available: Https://Danielmiessler.Com/Study/Security-By-Obsecurity/. [Accessed 23 July 2018].

156 Jsi, “About Us,” Jsi, 29 July 2018. [Online]. Available: Https://Www.Jsi.Com/Jsiinternet/About/Index.Cfm. [Accessed 29 July 2018].

157 S. Singh And S. Malhotra, “Data Warehouse And Its Methods,” *Journal Of Global Research In Computer Science,* Vol. 2, No. 5, Pp. 113-115, 2011.

158 Vincent & Jaquet-Chiffelle, Catherine & Coatrieux, Gouenou & Fassa, Maniane & Breton And F. Qantin, “Centralised Versus Decentralised Management Of Patients' Medical Records,” *Studies In Health Technology And Informatics,* Vol. 150, No. 10.3233/978-1-60750-044-5-700., Pp. 700-704, 2009.

159 B. M. Mutale And J. Phiri, “Web Based Document Archiving Using Time Stamp And Barcode Technologies - A Case Of The University Of Zambia,” *International Journal Of Innovative Research In Science, Engineeringand Technology,* Vol. 5, No. 4, Pp. 4625-4634, 2016.

160 M. A. King, “A Realistic Data Warehouse Project:An Integration Of Microsoft Access® Andmicrosoft Excel® Advanced Features And Skills,” *Journal Of Information Technology Education Innovations In Practice,* Vol. 8, Pp. 91-104, 2009.

161 S. Prakbhakar, S. Pankanti And A. K. Jain, “Biometric Recognition: Security And Privacy Concerns,” *Ieee Security & Privacy,* Vol. 3, No. 1540-7993, Pp. 33-42, 2003.

162 J. Corbett, “The Biometric Id Grid: A Country-By-Country Guide,” The Corbett Report: Open Source Intelligence News, 31 January 2017. [Online]. Available: Https://Www.Corbettreport.Com/The-Biometric-Id-Grid-A-Country-By-Country-Guide/. [Accessed 2018 August 13].

163 C. Mumba, “Mumba Yachi Arrested,” *Zambia Daily Mail,* Vol. 405730/10/1, No. Zn550035, Pp. 1-12, 2017.

164 G. Intelligence, “The Impact Of Privacy And Data Protection Legislation On Biometric Authentication,” Goode Intelligence, 2015.

165 M. S. Uddin And A. Y. Akhi, “Horse Detection Using Haar Like Features,” *International Journal Ofcomputer Theory And Engineering,* Vol. 8, No. 5, Pp. 1- 4, October 2016.

166 M. Mwiya, J. Phiri And G. Lyoko, “Public Crime Reporting And Monitoring System Model Using Gsm And Gis Technologies: A Case Of Zambia Police Service,” *International Journal Of Computer Science And Mobile Computing,* Vol. 4, No. 11, P. 207 – 226, November 2015.

167 Microsoft, “Bing,” Microsoft, [Online]. Available: Https://Binged.It/2obh3bk. [Accessed 3 August 2018].

168 Microsoft, “Tanzania Identity Card,” Microsoft, [Online]. Available: Https://Binged.It/2oajb9r. [Accessed 3 August 2018].

169 Unicef, “Unicef: For Every Child,” Un, November 2017. [Online]. Available: Https://Data.Unicef.Org/Wp-Content/Uploads/2017/12/Birthregformbotswana.Pdf. [Accessed 4 August 2018].

170 Microsoft, “Bostwana Identity Card,” Microsoft, [Online]. Available: Https://Goo.Gl/Images/H5n1n8. [Accessed 4 August 2018].

APPENDICES

Appendix 1: Countries with Biometric Identification and Authentication Systems.

In a country by country biometric ID report for 2017, James Corbett lists forty-two countries that have either implemented biometric ID systems that work as civil documents for identification and authentication or are in the process of implementing them [162]. Some of the countries listed are:

Afghanistan – developed in 2016 by the Afghanistan National Security Forces, the Automated Biometric Information System with fingerprint, iris, and facial scan capabilities has been deployed.

Albania – deployed in 2009, the biometric identity card which complies with ICAO (International Civil Aviation Organization) for civil standards contains an embedded chip that stores fingerprints and a digital photograph along with biographical information. ICAO generates principles and techniques of international air navigation and encourages planning and development of international air transport to ensure safety and growth.

Australia – Deployed in 2005 and also used for visitor tracking and student attendance monitoring for schools. The cards contain biometric data.

Bahamas – As of 2016, the Bahamas has been issuing biometric passports.

Bermuda – Starting 2016, Bermuda has been deploying biometric passports.

Bolivia – In 2009 Bolivia conducted elections via biometric identification systems. In 2016 a biometric census was conducted on all foreign individuals.

Bulgaria – since 2010 biometric identity cards and passports have been issued to citizens.

Brazil – Starting 2011, biometric identity cards and biometric election ID cards have been issued to citizens.

Canada - Iris scans are used to identify passengers.

Chad – Chad enrolls biometric details of refugees fleeing war-torn neighboring countries.

Chile – Starting 2013 multi-mode National ID and biometric passports have been issued.

China – From 2016 China has been using biometric enrolment for all foreign travelers.

Finland – Starting 2012 Finland introduced biometric residence permit cards.

France – Since 2009 biometric passports which collect digital photos and eight fingerprints have been used.

Germany –Biometric passports were introduced in 2005 and biometric residence permits in 2011, both of which require a biometric digital photograph and two fingerprints to be collected and stored on an embedded chip. Germany's identity card does require a biometric photo.

Greece – as of 2017 plans to introduce biometric ID systems were still being considered

India – fingerprinting and iris scanning are in use.

Iraq – starting 2016 a national identity card system that uses biometric identifiers has been in use.

Israel – Starting 2009 the Biometric Database Law was enacted to pave way for the implementation of a national biometric ID database.

Japan – Starting 2007 fingerprints and digital photographs from all foreign travelers are collected.

Kenya – In 2012 Kenya began biometric voter registration and. In 2015, a biometric registration system for all citizens aged 12 and over was implemented.

Kuwait – In 2015 a law requiring all citizens and visitors to submit to DNA testing for a national database was passed. No actual collection has been done.

Luxembourg – biometric passports with a chip containing a digital photograph, two fingerprints and an image of the holder's signature are issued.

Mexico – starting 2011 the biometric identification cards to all children between 4 and 17 years old have been issued.

Netherlands – Since 2009 the Netherlands has issued biometric passports containing an embedded chip with a digital photograph and fingerprints.

New Zealand – New Zealand's Inland Revenue Department deployed "Voice ID" in 2011 to register "customers'" voice prints and identify them in future interactions.

Nigeria – Plans to implement fingerprint and facial biometrics in the 2018 census were approved in 2017.

Paraguay – In 2009 New Identification ID Systems were rolled out by adding thumbprint and digital photograph.

Peru – to issue biometric passports.

Philippines – In 2014 the Commission on Elections announced that biometric registration would be mandatory for all voters in the Philippines.

Saudi Arabia – Since 2015 biometric details (including fingerprints) of all citizens and expatriates have been collected.

Sierra Leone – since 2017 biometric registration kits have been deployed to aid in biometric identification and authentication systems.

Appendix II: Research Participant Questionnaire

The University of Zambia

School of Engineering

AUTOMATION AND SECURE BIRTH CERTIFICATE REGISTRATION AND MANAGEMENT PROCESS BASED ON BIOMETRICS AND QR BAR CODES.

By Lubasi K. Musambo (2016145787)

Master of Engineering – ICT Security

For further details or any queries, kindly get in touch on 0966 381452, lubasimusambo@gmail.com.

Dear Respondent,

I am a student at the University of Zambia in my final stage pursuing a Master of Engineering – ICT Security. As partial fulfilment for the award of a Master's degree, I am conducting a baseline study on: **"AUTOMATION AND SECURE BIRTH CERTIFICATE REGISTRATION AND MANAGEMENT PROCESS BASED ON BIOMETRICS AND QR BAR CODES."**

You have been purposively sampled to provide information for the topic indicated above. The information being collected is purely for academic purposes as such, it will be treated with maximum

confidentiality. Subsequently, you are not supposed to indicate your name or any personal information that can lead to revealing of your identity.

Your co-operation will be greatly appreciated.

For more information queries in relation to the survey, you may wish to contact the following:

Research Supervisor: Dr. Jackson Phiri Jackson Phiri (jackson.phiri@cs.unza.zm) or

Assistant Dean: Dr. Erastus Mwanaumo (erastus.mwanaumo@unza.zm)

Lubasi K. Musambo (Mr)

Student Number: 2016145787

UNIVERSITY OF ZAMBIA

Section A BACKGROUND INFORMATION.

1. What is your sex?

☐ Male
☐ Female

2. What is your age?

☐ 20 -29
☐ 30 - 39
☐ 40 – 49
☐ 50 - 59
☐ 60 and above

3. Which part of Lusaka do you live in?

☐ Low density area
☐ Middle density area
☐ High density area

4. What is your level education?

☐ Grade twelve
☐ Certificate
☐ Diploma
☐ Degree
☐ Master's degree
☐ Ph.D

Others specify…….

5. What is your marital status?

☐ Single, never married
☐ Married
☐ Widowed

☐ Divorced
☐ Separated

6. What is your occupation status at your work place?

☐ Executive Officer
☐ Director
☐ Manager
☐ Supervisor
☐ Subordinate

Section B PUBLIC'S KNOWLEDGE LEVELS ON BIOMETRICS.

7. Have you ever heard about BIOMETRICS?

☐ Yes
☐ No

8. How did you know about BIOMETRICS?

☐ Through radio
☐ Through TV
☐ Through internet
☐ Friends

Others Specify……

9. What kind of work do you think BIOMETRICS perform?

☐ Medical use – hospital use
☐ Criminal management – Police and other law enforcement
☐ Provision of security services (Confidentiality, Integrity, Availability, Authentication, Authorization, Accountability)
☐ Government Statistics

Others Specify……

10. Where do you think YOUR BIOMETRIC data is kept (yours or your friends or colleague's)?

☐ At my chief Executive Officer's home
☐ At work on an unknown computer in a file
☐ On the internet
☐ Others specify ……

11. Does your Organisation have a BIOMETRIC FRAMEWORK within which to identify, store and use biometric data?

- ☐ Yes
- ☐ No

If yes please state the framework or model in place:

……

……

……

……

……

If NO please state why:

……

……

……

……

……

12. Are you aware about any ZICTA innovation to manage biometric data?

☐ Yes
☐ No

13. If yes, kindly specify some of the innovations you know.

……

……

……

……

14. Do you think the public is adequately informed on biometric data, its use and how it is kept in Zambia?

☐ Yes
☐ No

15. If not, what do you think ZICTA OR GRZ should do to improve on its role in facilitating development through ICTS?

……

……

……

……

Section C

PUBLIC'S ATTITUDE TOWARDS BIOMETRIC DATA USAGE FOR ICT4D

For each of the following statements (16-19) circle one of the options to indicate how you feel. The options are labelled 1 - 5.

SA = Strongly agree (with statement) 1

A = Agree (with statement) 2

N = Neither agree or disagree (with statement) 3

D = Disagree (with statement) 4

SD = Strongly disagree (with statement) 5

16. You support USE OF YOUR BIOMETRIC DATA for organisation information security objectives because:

	1	2	3	4	5
You are aware about its use	SA	A	N	D	SD
Of your needs	SA	A	N	D	SD
Of your expectations	SA	A	N	D	SD
Of your perception	SA	A	N	D	SD
Of your attitude	SA	A	N	D	SD
I don't support the idea of biometrics in any form	SA	A	N	D	SD

17. You do not support use of your BIOMETRIC DATA to meet information security services of your organisation because:

	1	2	3	4	5
You are not aware about its use and applications	SA	A	N	D	SD
Your needs are not satisfied	SA	A	N	D	SD
Your expectations are not met	SA	A	N	D	SD
Of your perceptions about the organisation	SA	A	N	D	SD
Of your attitude towards the organisation	SA	A	N	D	SD

18. Do you think that ZICTA must develop a storage framework for biometric data for the Zambian environment or would you prefer your organisation to store this data?

	1	2	3	4	5
Develop biometric storage framework	SA	A	N	D	SD
ZICTA MUST Store all biometric DATA	SA	A	N	D	SD
Organisations must share their biometric data with ZICTA	SA	A	N	D	SD
Organisation must use the ZICTA framework only but manage their data	SA	A	N	D	SD

19. How would you want you biometric data stored by your organisation?

	1	2	3	4	5
Through ISO standards (e.g. ISO/IEC 24745:2011)	SA	A	N	D	SD
ZICTA developed model	SA	A	N	D	SD
Proprietary to every Organisation	SA	A	N	D	SD

Thank you for your help!

Appendix II: System Validation Questionnaire

The University of Zambia

School of Engineering

AUTOMATION AND SECURE BIRTH CERTIFICATE REGISTRATION AND MANAGEMENT PROCESS BASED ON BIOMETRICS AND QR BAR CODES.

By Lubasi K. Musambo (2016145787)

Master of Engineering – ICT Security

For further details or any queries, kindly get in touch on 0966 381452, lubasimusambo@gmail.com.

Dear Respondent,

I am a student at the University of Zambia in my final stage pursuing a Master of Engineering – ICT Security. As partial fulfilment for the award of a Master's degree, I am conducting a baseline study on: **"AUTOMATION AND SECURE BIRTH CERTIFICATE REGISTRATION AND MANAGEMENT PROCESS BASED ON BIOMETRICS AND QR BAR CODES."**

You have been purposively sampled to provide information for the topic indicated above. The information being collected is purely for academic purposes as such, it will be treated with maximum

confidentiality. Subsequently, you are not supposed to indicate your name or any personal information that can lead to revealing of your identity.

Your co-operation will be greatly appreciated.

For more information queries in relation to the survey, you may wish to contact the following:

Research Supervisor: Dr. Jackson Phiri Jackson Phiri (jackson.phiri@cs.unza.zm) or

Assistant Dean: Dr. Erastus Mwanaumo (erastus.mwanaumo@unza.zm)

……

Part A: Bio Data - Please tick in the box as appropriate

1) **Sex:** **(a**) Male ☐ (b) Female ☐

2) **Age in years.**

(a)	18 – 22	☐	(d) 30 – 34	☐
(b)	22 – 26	☐	(e) 34 – 40	☐
(c)	26 – 30	☐	(f) 40 and above	☐

3) **Marital status**

(a)	Single	☐	(d) Separated	☐
(b)	Married	☐	(e) Divorced	☐
(c)	Widowed	☐		

4) What is your level education?

- ☐ Grade twelve
- ☐ Certificate
- ☐ Diploma
- ☐ Degree
- ☐ Master's degree
- ☐ PhD

Others specify……

5) Do you work within the ICT department or are apprised with ICT?

- ☐ Yes
- ☐ No

<u>Part B: ACCEPTANCE TO CAPTURE BIOMETRIC DATA.</u>

5. Have you ever heard about BIOMETRICS?

- ☐ Yes
- ☐ No

6. Are you willing to have your facial biometric data captured?

- ☐ Yes
- ☐ No

If yes, then please run the model with your details and proceed. If No then thank-you, no further action needed from you.

<u>Part C: EASE OF USE OF MODEL (Reliability, Usability, Performance, Portability)</u>

For each of the following statements (7-11) circle one (or multiple) of the options to indicate how you feel. The options are labelled 1 - 5.

SA = Strongly Agree (with statement) 1

A = Agree (with statement) 2

N = Neither agree or disagree (with statement) 3

D = Disagree (with statement) 4

SD = Srongly Disagree (with statement) 5

7. According to you, the learning curve for using this biometric model is:

	1	2	3	4	5
Very Easy to use	SA	A	N	D	SD
Easy to Use	SA	A	N	D	SD
Not Sure	SA	A	N	D	SD
Difficult to Use	SA	A	N	D	SD
Very Difficult to Use	SA	A	N	D	SD
I did not use the program	SA	A	N	D	SD

8. In your words, how would you rate the satisfaction level of using the model that you experienced in terms of the model meeting vital data capture.

	1	2	3	4	5
Very satisfied	SA	A	N	D	SD
Satisfied	SA	A	N	D	SD
Indifferent	SA	A	N	D	SD
Not Satisfied	SA	A	N	D	SD
Very unsatisfied	SA	A	N	D	SD

9. In your own words, would you recommend this model for government use in the operations of vital capture and collections?

	1	2	3	4	5
Strongly recommend	SA	A	N	D	SD
Recommend	SA	A	N	D	SD
Indifferent	SA	A	N	D	SD
Can't recommend	SA	A	N	D	SD

If you answered Strongly Recommend or Recommend, what are the best features of the programs according to you?

_____

_____

_____

……....

If you answered Indifferent or Can't recommend, what recommendations would you suggest?

_____

_____

_____

10. Would you like to work with the program more often?

	1	2	3	4	5
Yes, very much	SA	A	N	D	SD
Yes	SA	A	N	D	SD
Not Sure	SA	A	N	D	SD
No	SA	A	N	D	SD

11. How would you rate this model in meeting your job functions?

	1	2	3	4	5
Task Accomplishment is Quick	SA	A	N	D	SD
Improves my job performance	SA	A	N	D	SD
Model makes my work unnecessary complex	SA	A	N	D	SD
Personal biometric Data is secure	SA	A	N	D	SD

12. Make a comment on the program based on your experience with it.

_____

_____

_____

13. This facial biometric model is installed as follows:

a) Install python
b) Install OpenCV's Modifiied Boost Algorithm
c) Install Xampp control (for server simulation run)
d) Run Xampp Control click on config, select http.conf, and
e) locate 'AddHandler cgi-script .cgi.pl.asp
f) Add .bat at end of this
g) Save, exit editor

Python and xampp are dependent on Ms Windows Operating system in Use (the researcher has used Ms Windows 10 Home single Language – 2017. On this platform Xampp Control is at version 3.2.2, Python is at version 3.5 32bit).

Considering processes 13 a-g do you think the Facial Biometric Model is portable enough?

Yes ☐ No ☐

14. The facial software biometric requires the following hardware resources:

a) Computer with at least 4GB RAM,
b) Hard disk capacity of at least 500GB,
c) A web camera with a resolution of at least 0.9MP 16:9 (1280 x 720).

Do you think these requirements are too ambitious or difficult to source?

Yes ☐ No ☐

Part D: ALTERNATIVE MODEL

15. Is there an optional biometric model that you have used before that can perform the functions developed in this model?

☐ YES
☐ NO

If yes then please state the model

Appendix III: Selected Source Codes

1.

```
# Program: Facial Capture
# Env: python
# Date: 2018
# Name: Lubasi K. Musambo
# School of Engineering, MEng ICT Sec
# The University of Zambia

import cv2
import os
import random
import string
import mysql.connector
def assure_path_exists(path):
    dir = os.path.dirname(path)
    if not os.path.exists(dir):
        os.makedirs(dir)
print('###########  Calibrating Facial Construction ###########')
print('')
print('')
idinput = ''.join([random.choice(string.digits) for n in range(3)])
vid_cam = cv2.VideoCapture(0)
face_detector = cv2.CascadeClassifier('haarcascade_frontalface_default.xml')
pic_id = idinput
strcon = int(pic_id)
print(strcon)
con =
mysql.connector.connect(host='localhost',user='root',password='',database='brsys')
m = con.cursor()
m.execute("INSERT INTO birth_details (pic_id) VALUES ({})".format(strcon))
```

```
con.commit()
con.close()
count = 0
assure_path_exists("dataset/")
while(True):
    _, image_frame = vid_cam.read()
    gray = cv2.cvtColor(image_frame, cv2.COLOR_BGR2GRAY)
    faces = face_detector.detectMultiScale(gray, 1.3, 5)
    for (x,y,w,h) in faces:
        cv2.rectangle(image_frame, (x,y), (x+w,y+h), (255,0,0), 2)
        count += 1
        cv2.imwrite("dataset/face." + str(strcon) + '.' + str(count) + ".jpg",
gray[y:y+h,x:x+w])
        cv2.imshow('Vital Facial Reconstruction', image_frame)
    if cv2.waitKey(100) & 0xFF == ord('q'):
        break
    elif count>50:
        break
vid_cam.release()
cv2.destroyAllWindows()
```

2.

```
#Program:  Generate Vital Document, Apply Encryption, Generate QRCode, Batch
# Env: pHp, HTML, javaScript, batch filing
# Date: 2018
# Name: Lubasi K. Musambo
# School of Engineering, MEng ICT Sec
# The University of Zambia


<?php
require_once 'core/init.php';
$user = new User;
@$uf_name = $user->data()->f_name;
@$us_name = $user->data()->s_name;
if ($user->isLoggedIn()) {
}else{
  Redirect::to('index');
}
?>
<!DOCTYPE html>
<html dir="ltr" lang="en">
<meta http-equiv="content-type" content="text/html;charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0, user-
scalable=0, minimum-scale=1.0, maximum-scale=1.0">
<head>
<meta charset="UTF-8" />
<title>VR|Registration </title>
<base />
<?php include_once 'userheadfiles.inc'; ?>
  <script type="text/javascript" src="js/qrcode_gen.js"></script>
<script type="text/javascript">
function myFunction(){
```

```
  WshShell = new ActiveXObject("Wscript.Shell"); //Create WScript Object
  WshShell.run("c://xampp/htdocs/fc/run.bat"); // execute batch .exe files
}
</SCRIPT>
</head>
<body>
<?php include_once 'lcheader.inc'; ?>
<div class="web_wrapper_hm">
 <div class="nests">
  <div class="text">
<?php
if(@$_GET['r']){
 $er = @$_GET['r'];
 if ($er == 'er02') {
  echo "
<div class='myalert' id='desktop-only' style='background: #d32f2f;position: absolute;
opacity: 1;'>
        <span class='flaticon2-cancel29' style='font-size:1.4em;'></span> The Picture
format is not <b>Correct.</b></div>";
       }elseif($er == 's77601'){
        echo "
<div class='myalert' id='desktop-only' style='position: absolute;opacity: 1;'>
        <span class='flaticon2-check74' style='font-size:1.4em;'></span> Person added
<b>Successfully.</b></div>";
       }elseif($er == 's77603'){
        echo "<div class='myalert' id='desktop-only' style='position: absolute;
background: red; opacity: 1;'>
        <span class='flaticon2-cancel29' style='font-size:1.4em;'></span>Sorry! You
have <b>unprocessed</b> data</div>";
       }else{}}
 ?>
 <a href="train.bat"><button class="btn btn-warning">Calibrate Data</button></a>
```

```
      <a href="face_recog.bat"><button class="btn btn-success">Recognize
Face</button></a>

          <div class="row">

    <div class="col-lg-12">

         <div class='panel'>

              <div class='panel-body'>

             <div style="text-align:center;"><img src="images/logo.png" style="width:
50px; height:50px;"><br>

             <span style="font-size: 1.5em; "><b>Republic of
Zambia</b></span><br><h3>Vital Details</h3></div><br><br>

                    <?php

      if (isset($_GET['id'])) {

             $info = $_GET['id'];

       $query = DB::getInstance()->query("SELECT * FROM `birth_details` WHERE
person_id = '$info' AND flag = (1)");

      if ($query->count()) {

             foreach ($query->results() as $info) {

          $f_name = $info->f_name;

           $s_name = $info->s_name;

            $m_name = $info->m_name;

            $register_date = $info->register_date;

            $sex = $info->sex;

            $dob = $info->dob;

            $person_id = $info->person_id;

            $district = $info->district;

            $town = $info->town;

            $village = $info->village;

            $chief = $info->chief;

            $province = $info->province;

            $father_employ = $info->father_employ;

            $mother_employ = $info->mother_employ;

            $birth_hospital = $info->birth_hospital;
```

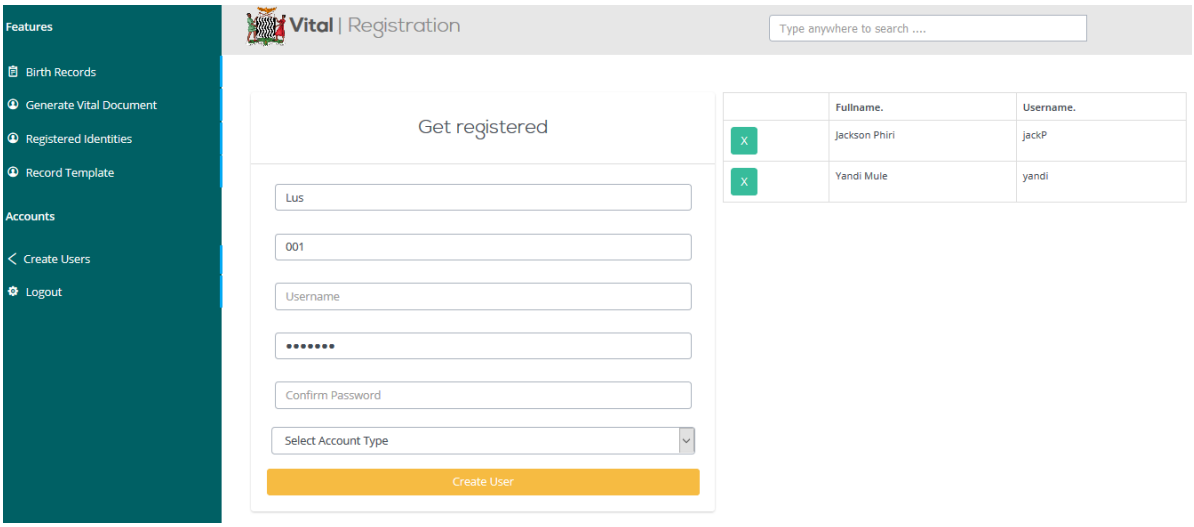
```
                $address = $info->address;
                $person_id = $info->person_id;
                $father_fname = $info->father_fname;
                $father_sname = $info->father_sname;
                $mother_fname = $info->mother_fname;
                $mother_sname = $info->mother_sname;
                $fa_nrc = $info->father_nrc;
                $mo_nrc = $info->mother_nrc;
                $bcert = $info->birth_cert_num;
                $mother_nrc = base64_decode($mo_nrc);
                $father_nrc = base64_decode($fa_nrc);
                 $dobenc = base64_decode($dob);
        $generate = rand(10, 30); //First Premium 6 users  ($_POST == $generate3)
        $generate2 = rand(30, 60); //Second Premium 12 users ($_POST == $generate2)
        $generate3 = rand(60, 90); //Third Premium 24 users ($_POST == $generate3)
        $gencode =
base64_encode($person_id.'/'.$father_nrc.'/'.$generate3.'/'.$register_date);
        $data = base64_decode($gencode);
                  $type ="Birth Certificate #:";
                $profile_pics = "<img src='face/dataSet/face.$person_id.3.jpg'
style='max-width:120px;max-height:120px;min-width:120px;min-height:120px;'>";
                $userdata = "<a href='#' class='button' id='btn-download'
download='my-file-name.png' ><span id='qrcode' class='pull-right'></span></a>";
                $infor = "<hr><h3>$f_name $m_name $s_name</h3><hr>
                      <ul class='list-unstyled'>
                        <li><b>Middle Name.</b> $m_name</li>
                        <li><b>Date of Birth.</b> $dobenc</li>
                        <li><b>Gender.</b> $sex</li>
                        <li><b>Registration Date.</b><br> $register_date</li>
                        <br>
                        <li><b>Registration Officer.</b><br> $uf_name $us_name</li>
```

```
                    </ul>
                    <hr><br>
                    <a href='nrc?id=$person_id'><button class='btn btn-
info'>Generate NRC</button></a> <a href='birth_cert?id=$person_id'><button
class='btn btn-warning'>Generate Birth Certificate</button></a>
                    ";
                }
            }else{
              echo "<div class='alert alert-info'>

        <strong>Sorry!</strong> This Individual does not exist.
       </div>";
            }
        }
    ?>
    <div class="col-lg-9">
    <?php echo @$profile_pics; ?>
     <?php echo @$infor;
     ?><br>
     </div>
    <div class="col-lg-3">
    <b><?php echo @$type; ?></b> <?php echo @$bcert; ?><br>
    <input id="qrcodes_map" type="hidden" value='<?php echo $f_name.' /
'.$s_name.' / '.$bcert.' / '.$register_date.' / '.$sex; ?>' /><br />
      <?php
      echo @$userdata;
    ?>
    </div>
        </div>
      </div>
     </div>
```

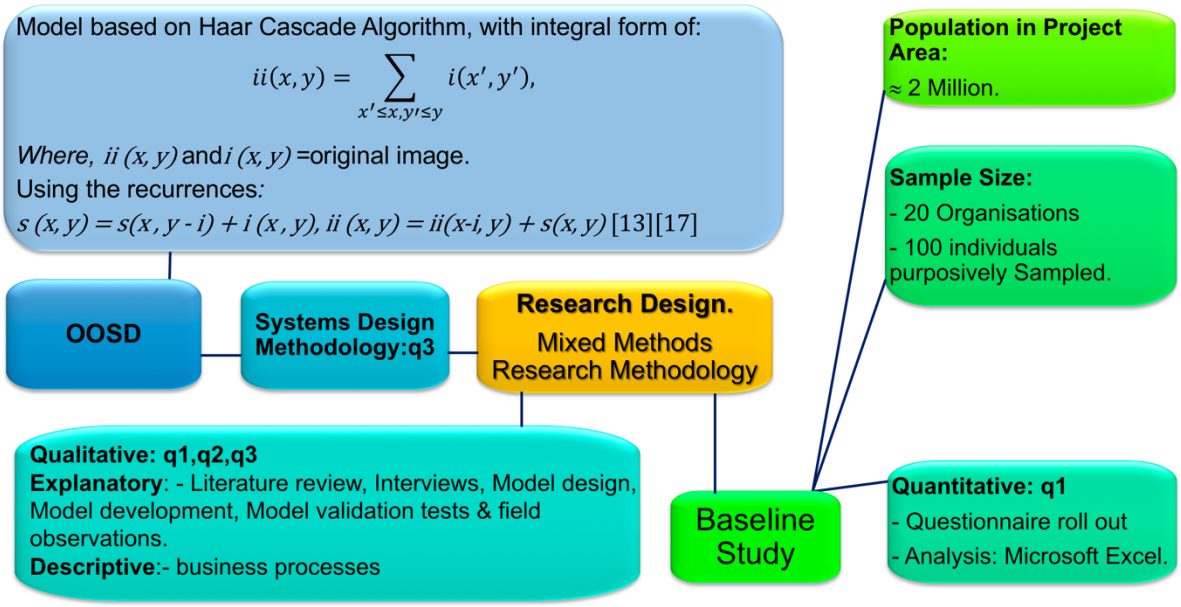
```
        </div>
</div>
</div>
</div>
<script type="text/javascript">
  // var qrcode = new QRCode("qrcode");
  var qrcode = new QRCode("qrcode", {
    width: 120,
    height: 120,
  });
function makeCode () {
  var elText = document.getElementById("qrcodes_map");
  if (!elText.value) {
    alert("Input a text");
    elText.focus();
    return;
  }
    qrcode.makeCode(elText.value);
}
makeCode();
var button = document.getElementById('btn-download');
button.addEventListener('click', function (e) {
    var dataURL = canvas.toDataURL('image/png');
    button.href = dataURL;
});
</script>
</body>
                                        </html>
```

Appendix IV: Creation of a New User on the System



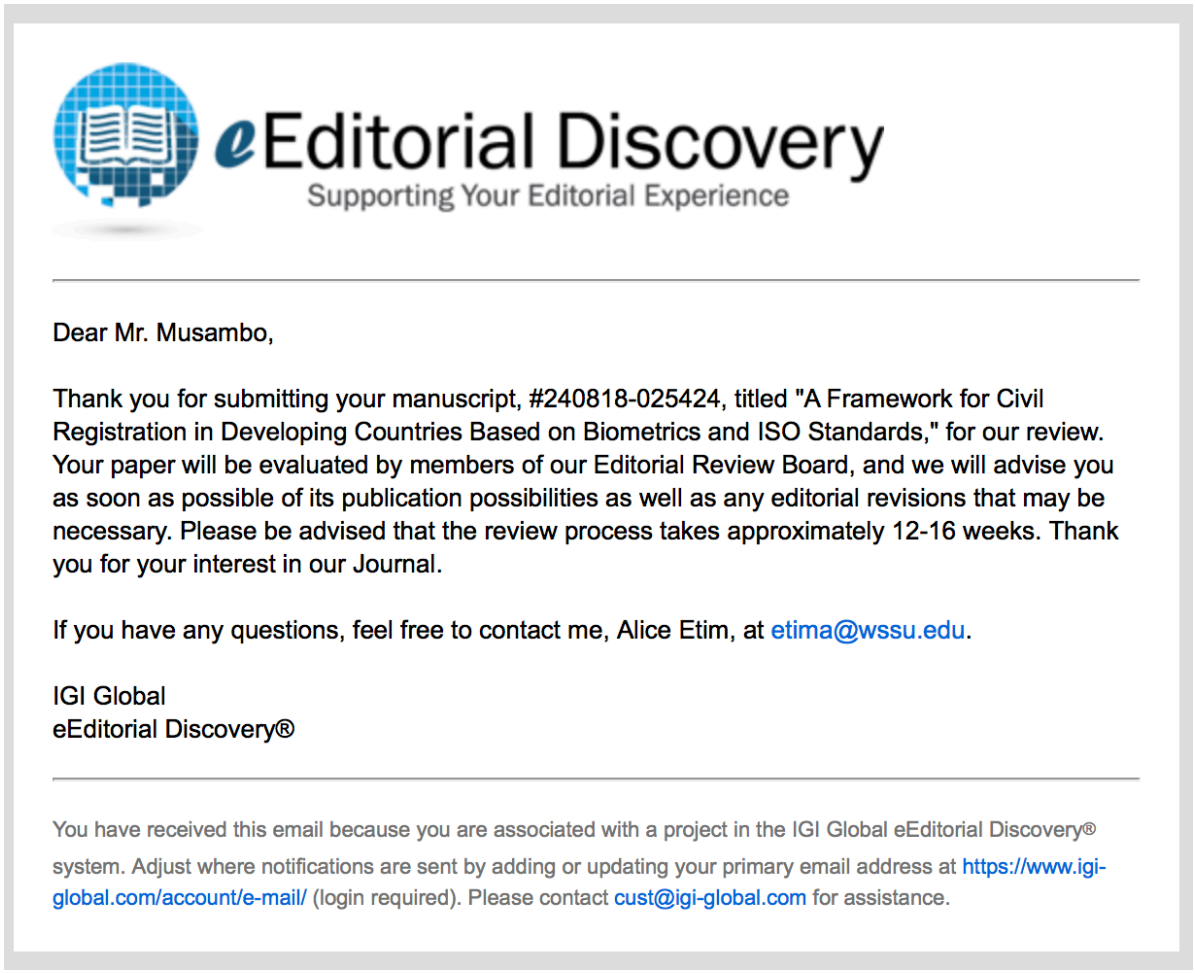
Create a new user by supplying needed credential data. User creation must be done using officer Region Number, and Man Number in username and a suitable alphanumeric password.

Appendix V: Project Mind Map



Appendix VI: Paper Acceptance Letters

1.



eEditorial Discovery
Supporting Your Editorial Experience

Dear Mr. Musambo,

Thank you for submitting your manuscript, #240818-025424, titled "A Framework for Civil Registration in Developing Countries Based on Biometrics and ISO Standards," for our review. Your paper will be evaluated by members of our Editorial Review Board, and we will advise you as soon as possible of its publication possibilities as well as any editorial revisions that may be necessary. Please be advised that the review process takes approximately 12-16 weeks. Thank you for your interest in our Journal.

If you have any questions, feel free to contact me, Alice Etim, at etima@wssu.edu.

IGI Global
eEditorial Discovery®

You have received this email because you are associated with a project in the IGI Global eEditorial Discovery® system. Adjust where notifications are sent by adding or updating your primary email address at https://www.igi-global.com/account/e-mail/ (login required). Please contact cust@igi-global.com for assistance.

2.

From: Bernard Banda
Sent: Monday, 30 July 2018 19:02
To: Lubasi Musambo; DL - Statistics&Research
Subject: RE: CALL FOR PAPERS:

Good evening

We would like to acknowledge receipt of the paper submitted. We will send comments after peer review within August 2018.

Regards

_____
From: Lubasi Musambo [lubasimusambo@gmail.com]
Sent: 30 July 2018 17:44
To: DL - Statistics&Research
Subject: CALL FOR PAPERS:

DEAR SIR
PLEASE FIND ATTACHED.

REGARDS

LUBASI K. MUSAMBO
Sent from Mail<https://go.microsoft.com/fwlink/?LinkId=550986> for Windows 10

_____
Bernard Banda Manager - Policy and Research
Head Office: |Stand Number 4909 Corner of United Nations Road & Independence Avenue|Lusaka - Lusaka
General Lines:+260 211 378200/ 241236/ 244426/ 246702/ 244427|Fax: +260 211 246701|Extension 8231
Mobile: +260 97 821 4329 Email: bbanda@zicta.zm Website:http://www.zicta.zm<www.zicta.zm>

[ZICTA LOGO] <default.asp>
A Regulator advancing the nation to a digital society through the values:
Integrity, Transparency, Innovation, Teamwork, Fairness, Excellence, Effectiveness & Accountability