Faculty of Computing and Informatics

Department of Informatics

DESIGNING MULTIMODAL BIOMETRICS FRAMEWORK FOR THE NAMIBIAN GOVERNMENT

Thesis submitted in fulfilment of the requirements for the degree of

Master of Informatics

at the

Namibia University of Science and Technology

Presented by:	**Licky Richard Erastus**
Student Number:	**200516450**
Supervisor:	**Dr Nobert Rangarirai Jere**
Co-Supervisor:	**Mrs Fungai Bhunu Shava**
Submission Date:	**December 2015**

DECLARATION

I, **Licky Richard Erastus** hereby declare that the work contained in this thesis presented for the degree of the Master of Informatics at the Namibia University of Science and Technology, entitled:

Designing Multimodal Biometrics Framework for the Namibian Government

is my original work, and that I have not previously, in its entirety or in part, submitted it to any other university or higher education institution for the award of a degree.

Student Name & Surname

Date

DEDICATION

This thesis is dedicated to my father, who taught me that the best kind of knowledge to have is that which is learned for its own sake.

It is also dedicated to my mother, who taught me that even the largest task can be accomplished if it is done one step at a time.

Lastly the thesis is also dedicated to my wife for her unconditional love and support.

ACKNOWLEDGEMENTS

I would like to extend my gratitude to the following people for their contribution to this research.

Firstly, I would like to thank my supervisors, Dr N. R. Jere & Mrs F. Bhunu Shava for their patience, continuous encouragement and guidance.

I also thank all the members and staff of the School of Computing and Informatics for their support.

Lastly, I am grateful to the experts that participated in this study and who contributed to the achievement of its objectives.

PUBLICATIONS ARISING FROM THE THESIS

Jere, N. and Erastus, L. R. (2015). An Analysis of Current ICT Trends for Sustainable Strategic Plan for Southern Africa. Proceedings of the IST-Africa 2015 Conference, Lilongwe, Malawi.

Erastus, L. R., Jere, N. and Shava, F. B. (2015). Exploring Challenges of Biometric Technology Adoption: A Namibian Review. Proceedings of the Emerging Trends in Networks and Computer Communications (ETNCC), 2015 International Conference. Windhoek, Namibia.

ABSTRACT

As technology evolves, the once reliable traditional authentication and verification systems are now open to a number of security threats, some of which may not be combated by these old or traditional security measures. For instance, Personal Identification (PIN) Numbers and passwords that are normally used to authenticate system users are vulnerable to shoulder surfing and systematic trial-and-error attacks. Cases have since been reported in Namibia in which people have lost personal belongings worth thousands of dollars as a result of information security breaches. In response to these security breaches, different technologies have been proposed with the aim to authenticate users, verify and or detect any possible fraud activities. Among these are firewalls, encryption and biometrics. Biometrics offer reliable identification mechanisms compared to other technologies due to their uniqueness and difficulty to be emulated. Regardless of the tremendous advances in biometric technology, the recognition systems based on the measurement of single modality (mono-modal) cannot guarantee 100% accuracy. Accordingly, multimodal systems based on multiple uncorrelated biometric signatures or traits offer more robustness in terms of recognition accuracy and handling of poor quality biometric samples.

The research used a qualitative research approach. For data collection, questionnaires, interviews, observations and document analysis were employed. A multiple case study strategy was used for data collection to ensure validity through data triangulation. Three Namibia ministries were selected as case sites as they are among the security critical sectors of the nation where the use of biometrics is imperative.

Results have shown that a number of biometrics is used in government departments in Namibia. However, the usage is still a bit low and a lot is required for citizens to trust and use biometrics. The major challenges in biometrics usage have been identified as a lack of technical skills, a lack of appropriate budget, too dynamic, social challenges and a lack of supporting policies. This study argues that even if these challenges are addressed, one biometric may not be reliable and very secure. The purpose of this research is to share possible biometrics that can be combined and used concurrently to address the identified security challenges. This saw the designing of a multimodal biometrics framework for the Namibian government.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1: RESEARCH INTRODUCTION

This chapter introduces the research and articulates the research background, problem statement, objective, and research methodologies. The analysis of the research's significance and research organisation is also included.

1.0 Introduction

This chapter introduces the research. It gives an overview of the research background by highlighting current developments in biometrics and security. The chapter goes on to explain the research problem statement and outlays the research question. From the research question, the chapter identifies research sub-questions and explains the overall objectives of the research. A review of the literature gives an account of how the research problem and research sub-questions were met. A brief overview of the research methodology that was used to meet the objectives of the study is also included. Ethical considerations that were made through the conduct of this study are also highlighted in this chapter. The chapter concludes with an overview of the research.

1.1 Research background

The latest inventions in biometric security have coincided with increased demand for better security at governmental level due to an increase in the population and crime. This is in such a way that Information and Technology (IT), through biometrics is seen as playing critical roles and among them being enhancing the implementation of national security, involving the upkeep of sensitive information and making sure that it is accessible to the right people from any location and assisting in the identification of individuals (National Science and Technology Council, 2011; UIDAI, 2010). Consequently, governments in developed and developing nations are moving towards implementing biometric security systems within their various ministries and departments (Unar, Seng & Abbasi, 2014; AADHAAR, 2010; Jain & Kumar, 2010; Mukhopadhyay, Muralidharan, Niehaus & Sukhtankar, 2013; National Science and Technology Council, 2011; UIDAI, 2010). Unar et al. (2014) have since noted that the biometrics industry revenues can increase from $(USD) 1,185 million in 2007 to a projected $(USD) 9,916 million in 2015 as a result of the growing interest from the Asia Pacific region as well as the Middle East and African countries. For instance, India's biometrics unique identification project, dubbed the "largest biometric database on the planet" aims to provide a way of identification to its billion plus population (Jain & Kumar, 2010). In addition, the provincial government of Andhra Pradesh in India implemented a biometrics payment system with the aim of bringing transparency and addressing corruption by ensuring that the government's social grants are allocated to the rightful people (Mukhopadhyay et al., 2013). Similarly, African countries are also engaged in the deployment of biometrics based systems, for example Nigeria's biometrics National ID Card scheme which will also work as a bank card, and a biometric based passport scheme in Ghana as well (Unar et al., 2014).

The implementation of biometrics systems is motivated by the fact that, the once reliable traditional authentication and verification systems are now open to a number of security breaches, some of which may not be combated by these old or traditional security measures. For instance, Personal Identification (PIN) Numbers and passwords which are normally used to authenticate system users are vulnerable to shoulder surfing and systematic trial-and-error attacks (Cho, Hwang & Park, 2009). Cases have since been reported in the United States of America and South Africa in which people have lost personal belongings worthy thousands of dollars as a result of security breaches (FBI, 2011; South African Financial Intelligence Centre, 2012).

However, the deployment of biometrics is characterized by numerous challenges that threaten their use in enhancing the security of already vulnerable systems. These challenges include social acceptance, performance, cost and poor infrastructures (Mukhopadhyay et al., 2013). Even though efforts have been made to address some of these challenges, with research proposing new and effective algorithms for biometric systems or proposing relatively inexpensive biometric systems, designing versatile and effective biometrics still faces a number of challenges which remain unaddressed (National Science and Technology Council, 2011).

1.2 Statement of problem

This section describes the research problem to be addressed. There are many problems associated with the biometrics implementation. Current literature indicates that in most cases unimodal biometrics possess a lot of challenges and may not be very efficient (Jain, Ross & Prabhakar, 2004). According to Jain et al, (2004), most of the biometric systems deployed in real world applications are unimodal, which rely on the evidence of a single source of information for authentication (e.g. fingerprint, face, voice etc.). These systems are vulnerable to a variety of problems such as noisy data, intra-class variations, inter-class similarities, non-universality and spoofing. As such the unimodal biometrics creates a lot of challenges, and at times, it is not very reliable to use.

The current challenges posed by unimodal biometrics motivate the need for multimodal biometrics systems. It is clear that there are also challenges involved with the multimodal systems (Jain et al., 2004). Multimodal biometrics systems combine biometric identifiers to obtain a more accurate decision on a user's claim, based on multiple sources of evidence. In a multimodal biometric system, each subsystem provides an opinion or a decision on the user's claim. This makes the implementation of multimodal biometrics more complicated and the need for proper planning (Jain et al., 2004). Hence, the present thesis focuses on the multimodal biometrics which offers high security options.

As such, currently there is no comprehensive plan or reference document for the government of Namibia on the multimodal biometric deployment. In addition, little research on biometrics has been done in Namibia and there are few reference documents on Namibian biometrics deployments. In this research, the different components that can affect the successful deployment of multimodal biometrics in Namibia are explained.

These form the basis of the problem statement that the research addresses. The major problems are illustrated in four aspects as shown in Figure 1.

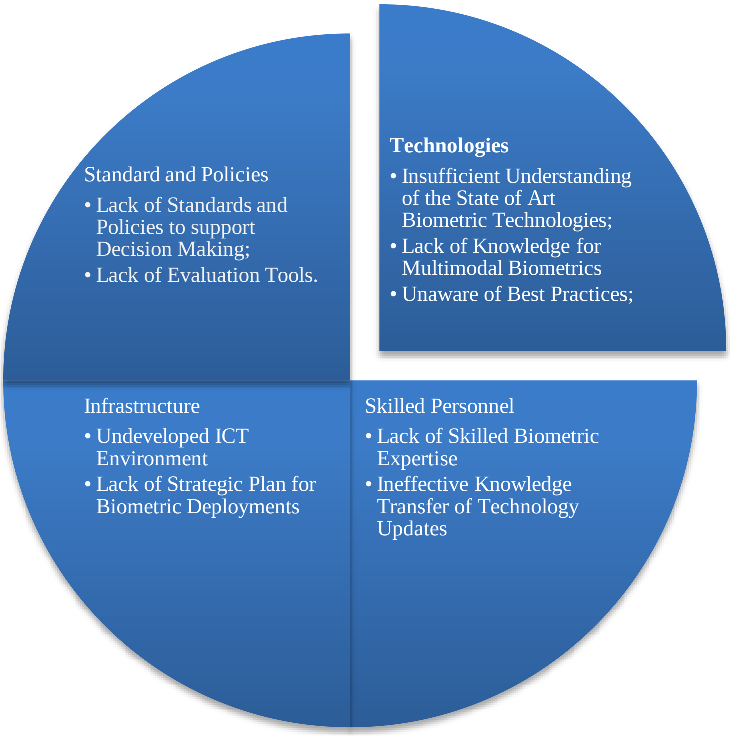

Standard and Policies
• Lack of Standards and Policies to support Decision Making;
• Lack of Evaluation Tools.
Technologies
• Insufficient Understanding of the State of Art Biometric Technologies;
• Lack of Knowledge for Multimodal Biometrics
• Unaware of Best Practices;
Infrastructure
• Undeveloped ICT Environment
• Lack of Strategic Plan for Biometric Deployments
Skilled Personnel
• Lack of Skilled Biometric Expertise
• Ineffective Knowledge Transfer of Technology Updates

Figure 1: Overview of research problem (Authors' perspective)

To address the research problem, the following research question and sub-questions were identified:

1.3 Research questions

The main research question of the thesis is outlined as follows:

> ***How can the Namibian government successfully prepare for multimodal biometrics deployments for different departments?***

The main research question is achieved by addressing the following sub-questions:

- How is the use of current biometrics in the Namibian context?
- What are the choices available to the government in terms of using multimodal biometrics technologies for security purposes?

- What are the key multimodal biometrics technologies that work for different government departments?
- What ICT infrastructure should be in place or is required to support multimodal biometrics deployment in Namibia?

1.4 Research objectives

The study aims to answer the research questions raised in the above section by designing a comprehensive framework for implementing multimodal biometric technologies that is suitable for the Namibian government. In addition, the study aims to:

- Identify the use of biometrics for the Namibian government.
- Establish different biometric traits that could be used in multimodal biometrics
- Identify multimodal biometrics technologies and related applications for government departments.
- Identify an ICT infrastructure to support multimodal biometrics deployment in Namibia.

These objectives can be achieved by an assessment of the challenges that exist and the lessons that can be learnt from the current implementations where biometrics are used for identification in government sectors both in Namibia and from other countries.

1.5 Research methodology and philosophical paradigm

This research subscribes to the interpretivist philosophy. The research makes use of a multiple case study approach to collect data to be used to meet the aims of the research. The multiple case studies are implemented within the interpretivist philosophy. Case studies are suitable for this study as the researcher has no control over the phenomenon under study (biometric deployment by the Namibian government) and the phenomenon cannot be studied outside the context in which it occurs **(**Yin, 2003**).** Triangulation (document analysis, questionnaire, observation and interviews) shall be used for data collection. The designing of the data collection instrument is guided by propositions in the literature, in particular the ICT roadmap theoretical framework proposed by Jere et al. (2012).

Data analysis is conducted through cross-case analysis. Open and closed coding is used for data analysis during the case analysis.

1.7 Significance/contribution

The framework in this thesis provides a suitable strategic plan for the government to design, implement and deploy multimodal biometrics systems that are suitable for the Namibian government.

The thesis produces a reference document that can be used by all biometrics systems stakeholders in Namibia.

Motivation of the research

In this research, the motivation is that the use of the multimodal biometrics systems has become one of the crucial concerns to the government of Namibia. The research studies the state of the art technologies and their best practices; analyses the challenges of the government of Namibia, and design a framework to support the decision-making on the planning of biometric deployments. The framework is aimed to be used as a reference tool by the Namibian government.

1.8 Research strategy and outcomes

This section shows how the research sub-questions of this study relate to each other. In addition, this section explains how these research sub-questions and objectives were addressed, and by which sections. Table 1 displays a summary of the sub-questions, their respective sub-objectives and the respective sections of this study that addressed them.

Table 1: Summary of research sub-questions and sub-objectives.

Research sub-question	Research sub-objective	Chapters or sections that addressed sub-questions and sub-objectives
How is the use of current biometrics in the Namibian context?	Identify the use of biometrics for the Namibian government.	Section 2.6 of Chapter 2 identified different uses of biometrics in the reviewed cases studies. Data collection and subsequent analysis of Chapter 4 (section 4.1) and 5 went on to reveal that, the Namibian government departments use multimodal biometric technologies for controlling physical access to premises, accessing personal devices, accessing personal information and the verification of information.
What are the choices available to the government in terms of using multimodal biometrics technologies for security purposes?	Establish different biometric traits that could be used in multimodal biometrics.	Chapter 2 of this research identified characteristics that define a biometric trait. Based on these characteristics namely universality, distinctiveness, invariance, collectability and performance, Chapter 5 and 6 established Namibian ministries can use biometrics traits namely fingerprint, face, iris, signature, hand geometry and DNA for its multimodal biometrics.
What are the key multimodal biometrics technologies that work for different government departments?	Identify multimodal biometrics technologies and related applications for government departments.	Chapter 2 of this study identified different technologies for multimodal biometrics. Data collection and analysis of Chapter 5 and 6 found that most ministries use AFIS system as their biometrics systems are fingerprint based.
What ICT infrastructure should be in place or is required to support multimodal biometrics deployment in Namibia?	Identify the ICT infrastructure to support the biometrics deployment in Namibia.	Chapter 6 shows that multimodal biometrics infrastructure namely a wide area computer network connecting all the departments and divisions involved, computer servers with database for storing templates, biometrics devices such as scanners and cameras, respective software that processes biometrics traits and electricity to power the infrastructure.

1.9 Thesis organisation

The thesis is organized as follows:

- Chapter 2 gives an overview of biometrics traits that can be used for multimodal biometric systems. The chapter evaluates technologies that can be used to facilitate multimodal biometrics. In addition, selected case studies are discussed to establish how biometrics can be deployed by governments and the private sector.
- Chapter 3 explains the research methodology used to address the research questions and to meet the objectives of the study. The research aims were met through data collection methods using a multiple case study approach within the interpretivist philosophy. The chapter also explains the precautions and procedures that were considered during data collection. Observation, document analysis, interviews and a questionnaire were used for data collection.
- Chapter 4 outlines the findings from all cases considered during data collection. Four ministries were considered during data collection. Findings for each case are outlined, supported by quoted statements and statistics from data gathered through interviews and questionnaires respectively. Data was outlaid within the aspects of the ICT roadmap theoretical framework.
- Chapter 5 presents a cross-case analysis of findings from all cases considered. These findings were also compared to previous findings in the available literature. Chapter five found technological aspects and issues on biometrics uses in the Namibian government, biometrics challenges (costs, interoperability, failure to capture prints, false rejection, lack of biometrics skills and knowledge, acceptance and use of biometrics, infrastructural challenges and other challenges), IT infrastructures for multimodal biometrics, biometric necessity, and the availability of a maintenance policy. Political and governance aspects found include biometrics stakeholders and policies.
- Chapter 6 derives components of the framework for multimodal biometrics implementation in the Namibian government from findings of chapter five. The components were identified based on the assessment on what challenges exist and lessons that were learnt from current implementation. The identified components include the multimodal ICT infrastructure; biometrics architecture and technologies; multimodal biometrics technical skills; social acceptance; biometrics stakeholders; biometrics budget; biometrics polices, implementation standards and plans; biometrics trends and emerging technologies; biometrics consultants/committees and biometrics monitoring, evaluation

and updating. Based on these components, chapter six proposes a framework for multimodal biometrics implementation in the Namibia government.

- Chapter 7 concludes the research. It revisits the research questions and sub-questions, and outlines what was done to address them. The main objective was met through designing a multimodal biometrics framework for the Namibian government.

1.10 Conclusion

The research targets the Namibian government departments where the security of citizens is essential. It is hoped that at the end of the research, a comprehensive research document will be available for the Namibian government. The proposed multimodal framework shall be used as a source reference for national biometrics deployments. A couple of approaches as mentioned in the methodology section were used. The techniques are determined and motivated by the current literature on biometrics. At the end of the research, a multimodal biometrics framework is designed.

CHAPTER 2: BIOMETRICS OVERVIEW

The chapter gives an overview of biometrics traits and respective technologies needed to support the biometrics. The chapter also pays reference to selected case studies to outlay possible deployments of biometrics and associated challenges.

2.0 Introduction

The once reliable traditional authentication and verification systems are now open to a number of security threats, some of which may not be combated by these old or traditional security measures. For instance, Personal Identification Numbers (PIN numbers) and passwords which are normally used to authenticate system users are vulnerable to shoulder surfing and systematic trial-and-error attacks (Cho, Hwang and Park, 2009). In response to these security breaches, different Information and Communication Technologies (ICTs) devices armed with algorithms have since been proposed with the aim to authenticate users, as well as verify and or detect any possible fraud activities. Accordingly, this chapter defines the term biometrics in particular reference to security and goes on to discuss different biometrics traits used for biometrics securities. It also articulates the implementation of biometrics securities and presents case studies on biometrics security usage, indicating their implementations and the challenges faced.

2.1 Definition of biometrics for security

Jamil (2011) proposes that biometrics include the automatic recognition and verification of individuals based on their physiological features such as finger prints, face, retina, iris, hand geometry and behavioural characteristics such as voice patterns, handwriting and keystroke dynamics. Today's more concentrated research efforts on biometric security solutions suggest a shift in security solutions based on what we know to what we have (Clodfelter, 2010). This is motivated by the advantages that human biometrics are different from one individual to the other. They make part of a human body, which implies that one cannot lose his or her biometrics and since they are a part of a human being, people do not need to memorise them, something that reduces chances of forgetting them or even getting stolen like in the case of passwords or security tokens (Canuto, Pintro and Xavier-Junior, 2013). The research community has since motivated the idea of human identification based on physiological or behavioural attributes of individuals, very often termed as “biometrics” (Seng, Unar and Abbasi, 2014). Physiological biometrics involve the automatic recognition of individuals through their unique physiological (finger-print, face, iris etc.) or behavioural (voice, gait, signature, typing behavior etc.) attributes (Cho et al., 2009; Clodfelter, 2010; Seng et al., 2014). Some of them are shown in Figure 2.

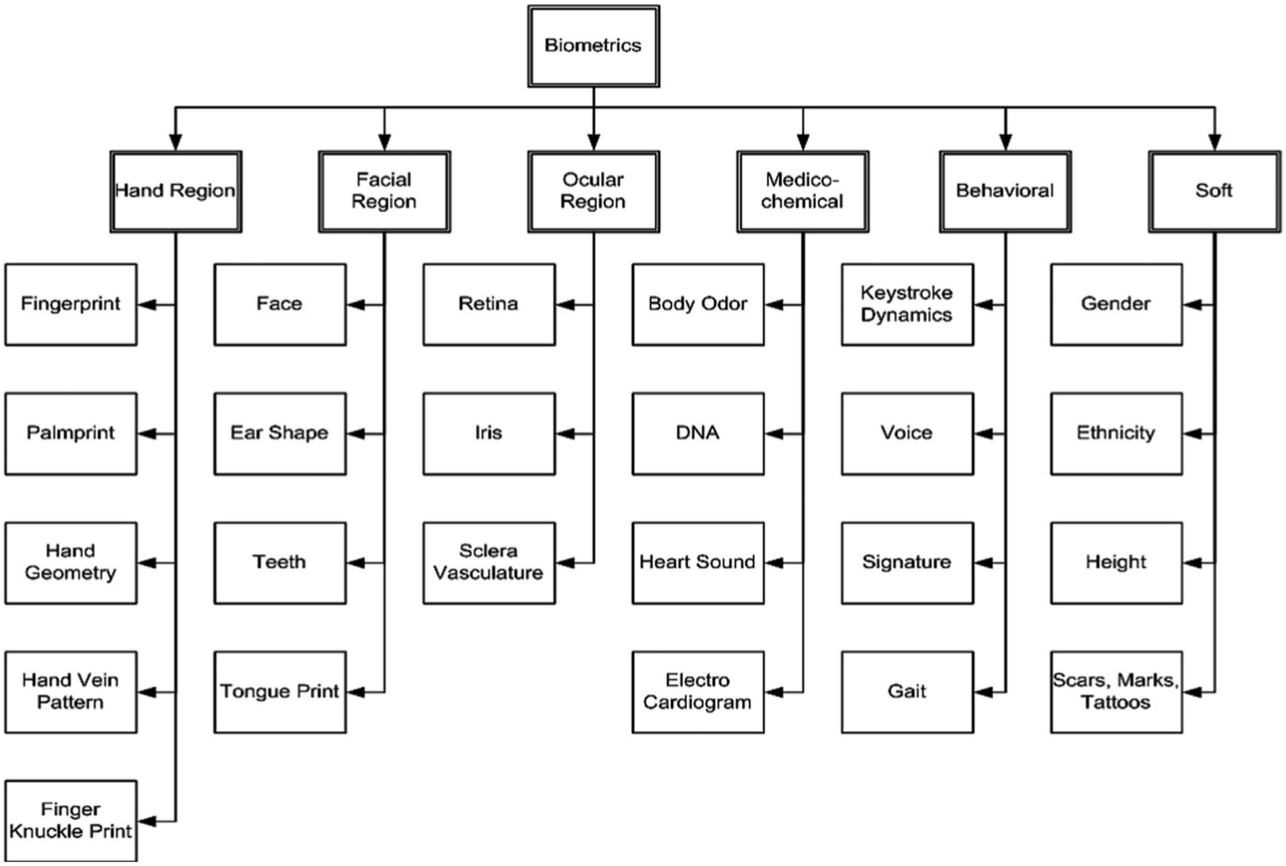


Figure 2: Classification of biometrics modalities (Seng et al., 2014).

Any physiological or behavioural attribute can qualify for being a biometrics trait if it satisfies the criteria such as:

I. universality: possessed by all humans,

II. distinctiveness: discriminative amongst the population,

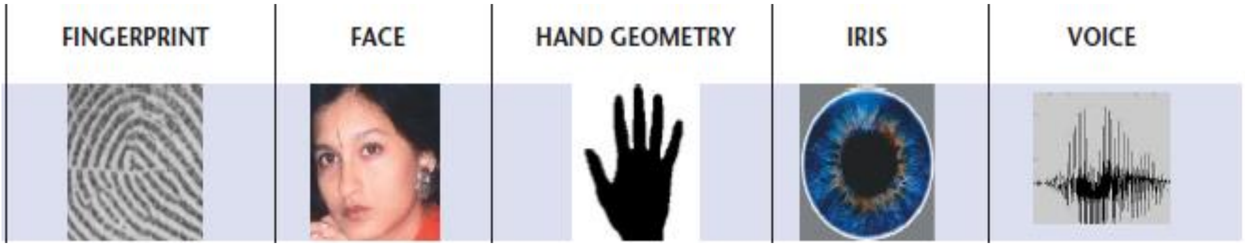
III. Invariance: the selected biometrics attribute must exhibit invariance against time,

IV. collectability: easily collectible in terms of acquisition, digitization and feature extraction from the population,

V. performance (Jain et el., 1998 cited in Bours 2012; Seng et al., 2014; Cho and Wang, 2006; Cho et al., 2009).

Table 2 shows examples of biometrics.

Table 2. Summary of biometrics traits (Salil, 2003)



An overview of some of the biometrics modalities shown in Figure 2 and Table 2 is done in the next section.

2.2 Modalities used in biometrics security

Biometrics are commonly used for security purposes to uniquely identify an individual (Darvaes, 2010). Biometrics can be defined as the automatic recognition and cross checking of a person based on the visible features (Jamil & Muhammad, 2011). Biometrics are physical characteristics making up inherited traits that come out as a person grows (Jamil & Muhammad, 2011). Examples include most of the body parts such as: fingerprints, face, iris; and hand geometry, individual voice, handwriting, and keystroke dynamics. These biometrics modalities are discussed below according to the regions where they are found on a person's body.

2.2.1 Hand region modalities

2.2.1.1 Finger print - Finger prints are print patterns that result from human fingertips, ridges and valleys. They are unique and develop during pregnancy. Studies have proven that people cannot have the same fingerprints (Maltoni, Maio, Jain, & Prabhakar, 2003). Finger prints have been used for more than 100 years in forensics hence their use is well developed (Clodfelter, 2010).

Nevertheless, injuries to fingers like burns, cuts and bruises can temporarily damage the quality of fingerprints but the patterns are restored once these injuries are fully healed.

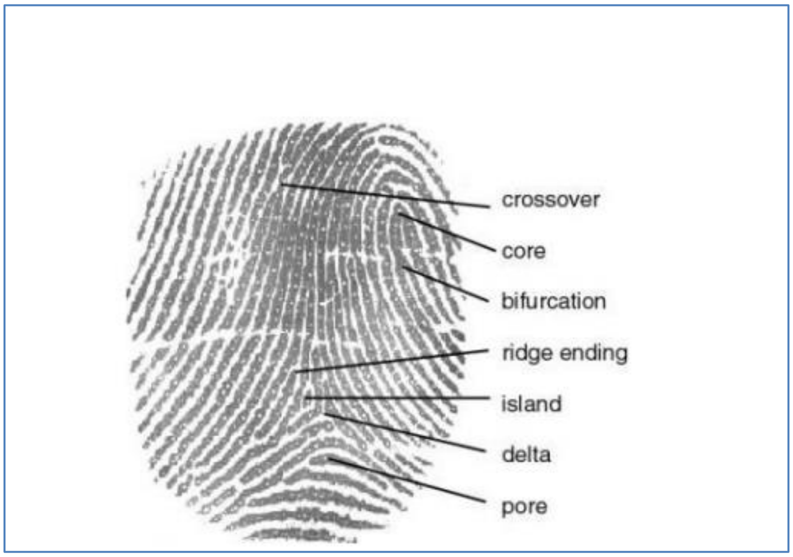


Figure 3: A sample finger print image showing different ridge patterns and minutiae types (Unar, Seng & Abbasi, 2014)

ICT technologies used in biometrics security for finger print - A finger print recognition system uses the texture of ridges and valleys present on the finger tips whereby the ridge endings (minutiae points) perform the recognition task and the ridge flow classifies the finger prints into one of the five categories such as arch, tented arch, left loop, right loop and whorl (Seng et al., 2014).

Common technologies used for finger prints are as follows:

I. **Solid State Scanners**: is a live-scan fingerprint scanner that measures some physical property of a fingerprint and converts it to a digitized ridge-valley image.

II. **Optical Scanners -** These devices map the 3D fingerprint on the electro optical currency and it is very difficult to cheat using a photograph or a printed image.

III. **Ultrasound sensors** are designed through sending acoustic signals towards the fingertip and capturing the echo signal which is then used to compute the ridge structure of the finger with a transmitter. The sensor then generates ultrasonic pulses and a receiver will detect reflected sound signals from the surface of the finger. A key advantage of ultrasonic scanners is that they are resilient to all forms of dirty accumulations on the fingerprint surface and produce quality images.

IV. **Pressure based fingerprint scanner**. It is the most common fingerprint scanner that requires one to have complete contact with sensor surface for the finger prints to be scanned or captured (Wasserman, 2005). This implies that fingertip skin dryness, skin disease, dirt and humid air may negatively affect ideal contact when using pressure based fingerprint scanners.

2.2.1.2 Palm print - Kekre, Sarode and Tirodka (2011, p. 31) propose that the “palm print, which is the inner surface of the hand possesses certain discernible and unique characteristics which can be easily extricated using a Palm print Capture Device”. Kekre et al. (2011, p. 31) further add that “these unique characteristics include principal lines, ridges, minutiae points, singular points and texture”. In addition, research by Connie, Jin, Ong and Ling (2005) supports these propositions by suggesting that palm prints can be used to uniquely identify human beings as they cannot be duplicated across different people, even in twins. Figure 4 shows the palm’s unique characteristics. Palm print recognition is used in civil applications, law enforcement and many such applications where access control is essential (Sumalatha & Harsha, 2014). However, people’s palm prints are prone to “imposter attacks and impersonation” as people touch various objects from which the prints can be harvested (Kumar, Garg & Hanmandlu, 2014). Palm prints can also be harvested while one is asleep or unconscious, thereby increasing chances of personation.

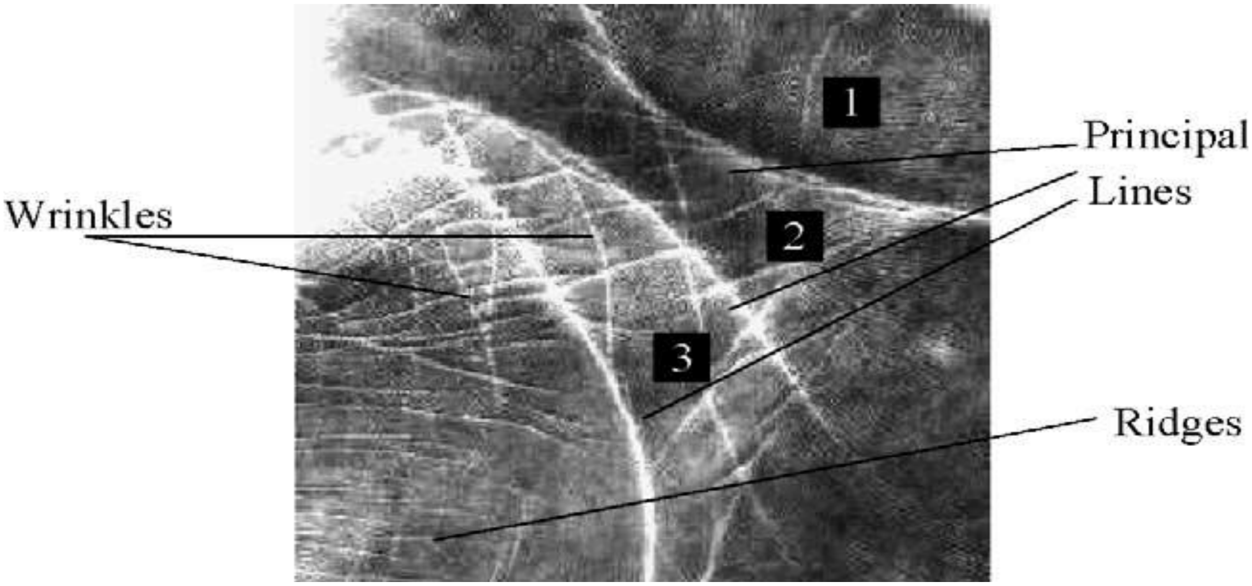


Figure 4: Palms' unique characteristics -"The three principal lines: 1-heart line, 2-head line and 3-life line" (Zhang et al., 2003 cited in Connie et al., 2005).

ICT technologies used in biometric security for palm print **-** different sensor types - capacitive, optical, ultrasound and thermal can be used to collect the palm digital image (Kekre et al., 2011). Thus, (Charge-Coupled Device) "CCD-based scanners, digital scanners, video cameras and tripods can be used to collect palm print images and provide high resolution images and align palms accurately because it has pegs for guiding the placement of hand" (Sumalatha & Harsha, 2014, p. 431). On the other hand, digital scanners are coupled with poor image resolutions and are too slow for real time scanning system set-ups (Sumalatha & Harsha, 2014).

2.2.1.3 A hand vein recognition system – this utilizes the vein bifurcations and endings beneath the skin of the human hand (Kumar and Prathyusha, 2009, cited in Seng et al., 2014). Seng et al., (2014) noted that recent trends indicate more interest in vein technology as compared to other hand based modalities because they cannot be easily forged. According to Sathish, Saravanan, Narmadha and Maheswari (2012), hand vein biometrics has the following advantages:

I. **Live body identification**: Thus, it is only applicable to live a body; a non-live hand cannot be read and taken.

II. **Internal features:** less prone to wear and tear or the dryness and wetness of the hand surface since the system extracts the vein pattern from the inside of a hand rather than outside features.

III. **Non-contact:** there is no direct contact between hand vein recognition systems or devices and the hand being from where the vein pattern is extracted.

IV. **High security:** it constitute of a high level of distinctiveness.

***ICT technologies used in biometrics security for hand vein* –** Near-infrared rays' vein recognition systems are some of the technologies that can be used for capturing hand veins for biometrics use. Such technologies can capture the finger or wrist or palm vein.

2.2.1.4 Hand geometry – this takes into account the length, width, aspect ratio of fingers or palm as well as the length, thickness, area, skin folds and crease patterns of the human hand (Seng et al., 2014). Clodfelter (2010) noted that hand scanners have high accuracy rates and non-intrusiveness makes them popular even though they are expensive.

***ICT technologies used in biometric security for hand geometry* -** hand geometry systems make use of a camera to acquire a 3D image of the human hand. The image captures the top surface and side of a hand from which obtained data or information can be processed.

2.2.2 Facial region modalities

The most common facial region modality is the face. The face is discussed below as a biometric modality.

2.2.2.1 Face recognition - Face recognition is the most natural biometric trait used to recognize fellow beings since centuries. It uses facial features like eyes, nose and mouth as biometric traits. However, the non-linear structure of a human face makes it complex for pattern recognition and 3D facial recognition is expected to solve this problem. Still, systems cannot guarantee reliable identification in the presence of artifacts such as the application of cosmetics and plastic surgery (Seng et al., 2014). Moreover, a person's face may change or be changed over time, which may have a significant impact on the accuracy of such systems (Seng et al., 2014). High identification error rates as high as 20% in indoor settings and 50% in outdoor settings have already been noted (Clodfelter, 2010).

2.2.3 Ocular region modalities

This region possesses the most accurate, highly reliable, well protected, stable and almost impossible to forge biometric signatures, for instance, retina, iris and sclera vein pattern (Seng et al., 2014).

2.2.3.1 A retinal identification system takes into account the unique and invariant structure of blood veins present on the human retina to establish the identity (Seng et al., 2014). In fact, a retinal scan system establishes the identity by examining either the landmarks (position and bifurcations of blood vessels) or measuring the area of reference (fovea, optic disk) (Seng et al., 2014).

2.2.3.2 Iris scanners use unique features of the eye such as the iris, which consists of crypts, furrows, corona and freckles (Clodfelter, 2010; Seng et al., 2014). Measuring the patterns of these features and their spatial relationships to each other provides other qualifiable parameters useful to the identification process (William, 2001). "Iris features can be acquired from a distance of 4 - 24 inches and require users to look calmly into a camera for quite some time before the analysis is complete" (Clodfelter, 2010, p. 182). Irises have the advantage of being "extremely distinctive", so as a result iris scanners are considered as "one of the most promising biometric tools" (Fowler, 2003 in Clodfelter, 2010, p. 182).

2.2.4 Behavioural biometrics modalities

2.2.4.1 Signature Dynamics - Is based on a handwritten signature to confirm one's identity. Dynamic signature verification increases computer security as well as trusted document authorization. The IT governance Institute (2004) states that there are two types of signature verifications namely: "simple signature and dynamic signature verification". Simple signature verification only verifies the signature while the dynamic signature verification considers many things about the signature such as speed of typing, timing, and placement of characters, as well as pressure applied to the pen.

2.2.4.2 Voice Recognition - Voice Recognition biometrics systems are based on one's pattern of speech (Khitrov, 2013). It is also known as speaker recognition as it "identifies and verifies a person on the basis of his or her unique voice characteristics" (Khitrov, 2013, p. 9). Clodfelter (2010, p. 182) concedes that "voice recognition works by measuring the distinct intonation, pitch, and pronunciation of an individual's voice and comparing those characteristics to a stored template". Features like one's "trachea, the nose, the placement of teeth, as well as the way a person accentuates sounds contribute to the uniqueness of one's voice" (Khitrov, 2013, p. 9). Khitrov (2013) further concedes that these characteristics in combination are as individual or unique as fingerprints and are non-transferable.

The main advantage of the voice biometrics trait is that there is no need for one's physical presents in order to take voice prints. Because of this advantage, Khitrov (2013) is of the view that voice biometrics can be used at call centres and interactive voice response systems (IVRs) and reduce customer delays during verification processes that are currently characterised by many question and answer segments. Additionally, the voice biometrics is simple and can be easily delivered through mentioning a phrase or saying a statement. Nevertheless, voice biometric traits have the following disadvantages that affect its accuracy or performance:

I. Environmental noise.

II. "Presentation effects, including speech sample duration, the physiological state of the speaker (e.g illness, emotions), and effects of vocal strain" (Khitrov, 2013 p. 10).

III. "Channel effects, including interference and distortion (e.g. frequency response, channel encoding)" (Khitrov, 2013, p. 10).

2.3 Implementation of biometrics systems

According to Barde, Khobragade and Singh (2012), biometrics systems can be classified into unimodal and multimodal biometrics systems. The unimodal biometrics system utilizes a single biometrics feature including either a physical or behaviour trait to identify and verify the user (Barde et al., 2012). Normally, the unimodal biometrics system is often used in a single functional system based on the fingerprint or face or iris or other biometrics features (Barde et al., 2012). Furthermore, this method is a mature technology and user friendly as it has been approved for several decades. For example, the fingerprint identification system has been utilized in criminal investigations for nearly one century, owing to its high accuracy, long-term stability and tenprint support to strengthen the ability of anti-spoofing.

However, some biometrics traits may change over time due to growth, aging, dirt and grime, injury and subsequent regeneration; and some of these unimodal biometrics systems are vulnerable to various issues such as noise, data and inter-class similarities (Latifi & Solayappan, 2006). Consequently, not all the unimodal biometrics systems have the same level of accuracy and performance. Compared with the weaknesses of the unimodal biometrics system, another type of biometrics system called the multimodal biometrics system has been widely used to overcome the limitations of the unimodal one and to achieve high recognition accuracy and performance. Multimodal biometrics systems are used to combine at least two differently independent biometrics sources of one person captured by different sensors.

Regardless of the tremendous advances in biometrics technology, the recognition systems based on the measurement of a single modality (mono-modal) cannot guarantee 100% accuracy (Seng et al., 2014). Accordingly, multimodal systems based on multiple, uncorrelated biometrics signatures or traits offer more robustness in terms of recognition accuracy and the handling of poor quality biometrics samples. Asmuni, Sim, Hassan and Othman (2014) recently demonstrated that using the iris and face offers considerable improvement to the accuracy by providing the extra complementary information and to resolve the limited discrimination capability, especially when compared to the uni-modal recognition approach. Seng et al., (2014) proposed that multimodal biometrics systems can be deployed in two different modes:

I. Serial/cascaded mode: the acquired multiple traits are processed one after another. The output of one trait serves as an input to the processing of the next trait.

II. Parallel mode: multiple modalities are processed simultaneously and the obtained results are combined together to obtain a final match score.

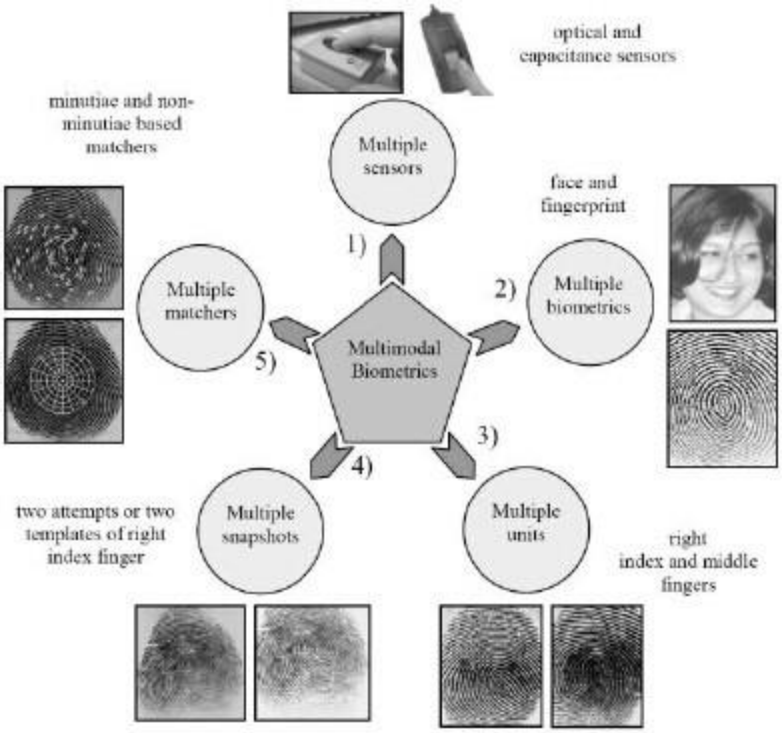

optical and capacitance sensors
minutiae and non-minutiae based matchers
Multiple sensors
1)
face and fingerprint
Multiple matchers
2)
Multiple biometrics
Multimodal Biometrics
5)
3)
4)
two attempts or two templates of right index finger
Multiple snapshots
Multiple units
right index and middle fingers

Figure 5: Diagram of Multiple Biometrics (Gudavalli, Babu, Raju and Kumar, 2012 cited in Seng et al., 2014).

2.4 Key areas of usage of biometrics

Biometrics security can be used anywhere where there is a need for the authentication or verification of participants. For example, it can be used for screening people receiving any form of aid or support from the government that can come in the form of food aid, fertilizers, seeds for farming, petrol, financial support for the old or social welfare support or even those in the rural areas receiving government subsidies (Sharma, ShivaKumar, Srinidhi & Kumar, 2014; Mukhopadhyay, Muralidharan, Niehaus & Sukhtankar, 2013). Biometrics security has also allowed for the distribution of banking facilities in rural areas through the use of agents where it is not economically feasible to setup a bank of brick and mortar.

In addition, biometrics can be used in government departments where there is a need for security and strict authentication like hospitals, army offices or quarters, the police, prisons, home affairs or banks, private offices and establishments where there is a need for authentication.

In India, biometrics security systems are used to curb corruption in the distribution of government services to the populace. The set up or uses always depends on the facilities and establishments that the government has.

2.5 Multimodal biometrics implementation process

Biometrics equipment is usually implemented in a centralized, managed and controlled environment. For example, the servers and nodes that are used to the capture data for authentication is housed within the same complex or department where the actual verification is to be done. However, there is a need for some form of management at every point where individual data is captured so as to control the action with respect to the outcome, for example granting access if the supplied data matches the stored template.

In addition, technology advancements now allow for the implementation of biometrics authentication in different ways. For example, the invention of the biometrics smart card with memory space for storing an encrypted template used to evaluate participants or individuals means that there is no need for setting up a networked environment with a server that stores template data that will be used when comparing with the supplied sample for authentication. Rather, the host device will simply evaluate an individual using template data stored in the biometric smart card against the supplied data/template (Sharma, ShivaKumar, Srinidhi and Kumar, 2014; Smart Card Alliance, 2011).

2.5.1 Onsite implementation of biometric securities

The biometric system can work in two modes: the enrolment and verification or the authentication mode.

2.5.1.1 The enrollment phase - samples of users or potential users are captured into the system and stored in the database. These samples are used to create a template that will be used as a source of reference once one uses the biometrics system for system access. The number of samples depends on the modalities being captured. For instance, high accurate modalities like finger prints may require a single capture of the sample, while voice recognition may need more than one sample to create a template per individual. Once a template has been created, it is stored in the database .

2.5.1.2 Verification phase - at this stage, an individual's biometrics traits are captured by a scanner or camera and compared with the template in the database to verify the identity. Once a match is found, access will be granted. However, failure means the individual is not recognized and cannot be granted access to system resources.

2.6 Case studies on biometrics usage and associated challenges

2.6.1 Case 1: Use of Voice Biometrics in the Health sector

Gold (2013), Beranek, (2013) and Khitrove, (2013) have demonstrated that voice biometrics can be effectively used in the health sector for patient and staff verification. The invention of mobile devices, cloud computing and the rise of bring-your-own-device (BYOD) technologies in the healthcare environment threatens the security and privacy of patient information. According to a February 2012 study by the US Government's Department of Health and Human Services (HHS), around 1.5 million Americans fall victim to medical identity theft each year, a number that could be far greater since most of the victims are unaware they have been a victim until several years later (Gold, 2013). These data breaches involve the theft or loss of mobile devices. In response to these security breaches, health centres like hospitals have implemented voice biometrics systems to authenticate both its staff and patients. The impact and popularity of voice biometrics cannot be doubted in the health sector as Julia Webb, VP of sales and marketing of one of a company that supplies voice biometrics noted that, her company is now delivering voice signature technologies to three of the top five US based health insurance organisations, which combined, cover 174.6 million people (Gold, 2013). Beranek, (2013) noted that common smart device ICTs can have voice biometrics implemented on them. Such voice biometrics include voice applications (Voice Apps) for authentication like Siri, Google Now and Samsung S Voice.

2.6.2 Case 2: Andhra Pradesh Provincial Government's (India) experience

Since independence, India has been embarking on alleviating poverty through state-sponsored schemes aimed at inclusive growth among its citizens. However, leakages throughout the state's implementation structure has restricted the ability of the Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS) and other social programs to reach target populations, resulting in a substantial volume of un-delivered benefits (Niehaus & Sukhtankar, 2012 as cited in Mukhopadhyay, Muralidharan, Niehaus & Sukhtankar, 2013). To overcome these challenges, among them corruption, the government integrated technology into the delivery of the government benefits. The technology in the form of the electronic benefit transfer (EBT) systems is coupled with the point-of-transaction service (PoS) biometrics authentication (confirmation of a user's identity through fingerprint reading or retinal scanning).

The whole system of government beneficial system involves the government and private sector. Banks must open savings accounts for all beneficiaries and regularly remit funds from the state by electronically crediting these accounts (Mukhopadhyay et al., 2013). Given that the program or scheme targets the poor in the rural area where it is not feasible to set-up a bank, the challenge lay on designing the appropriate payment delivery structure. Accordingly, the government introduced what they termed the "BC model". Simply put, a BC is an umbrella term referring to either an individual or organization that acts on behalf of a bank. Through a system of branchless banking stations, BCs extend financial services at a local level, including the management of small value deposits, the collection of interest on loans, the sale of micro-insurance products, and in the case of the Smartcard program, provision of EBT services" (Mukhopadhyay et al., 2013). At the lower end, local agents known as customer service providers (CSPs) are responsible for disbursing government beneficial funds. In order to execute a transaction, a CSP swipes a user's Smartcard in a PoS device that contains downloaded payment data (Mukhopadhyay et al., 2013). The CSP scans the user's fingerprint on the PoS reader in order to confirm a match and then disburses the cash payment with a receipt (Mukhopadhyay et al., 2013).

2.6.2.1 Description of operation

Even though the implementation is not uniform since it includes different banks, TSP, BCs and the government, the following procedures are normally followed:

I. Enrolment phase: vetted beneficiaries are enrolled into the system by TSPs/BCs according to different government beneficiary schemes. Operators use a netbook attached with a finger-print reader and a camera for capturing a photograph of a potential beneficiary.

II. Potential beneficiaries' details are uploaded to the TSP's central service using radio services (GPRS) technology or smart phones for banks to access the details. The bank authorises the opening of the account for each successful beneficiary.

III. Once enrolment is done, beneficiaries are issued with personalized smartcards by the TSP or an outside vendor.

IV. For payments, each GP is supplied with a smartcard reader – a POS device that has a slot for swiping a Smartcard, a fingerprint reader, a display screen, and a printer for generating receipts.

V. Execution of payments: the CSP must access the electronic payment file by syncing the POS machine with the main server and beneficiaries' smart cards, and finger prints are used for authenticity. Once this biometrics matches the ones in the system, payment is granted and the amount is deducted from the bank balance.

2.6.3 Case 3: Indian government's Aadhaar/Unique Identification Document (ID) project

With a population of more than a billion, the Indian government faced challenges in delivering welfare services to its populace. This was down to challenges with identification and high levels of corruption among other challenges (UIDAI, 2010; Mukhopadhyay et al., 2013). To address these challenges, the Indian government embarked on a project of allocating its citizens a unique biometric identity since 2006. The project was initially conceived by the Planning Commission as an initiative that would provide a clear and unique identity number for each resident across the country and would be used primarily as the basis for the efficient delivery of welfare services (UIDAI, 2010). Several studies consider India's unique ID project as a reference case study on the implementation of biometrics at government level. For instance, Zelazny (2012) recently conducted an evaluation of India's unique ID project with the aim to draw lessons from the case study and establish implications for other developing countries. Among other factors, India's unique ID project is believed to have created the largest biometrics database on the planet and on its successful completion, it is expected to become a model of a very large-scale usage of biometrics in electronic governance (Jain & Kumar, 2010).

In order to manage the implementation of its unique ID project, the Indian government created a statutory body, the UIDAI that had the responsibility of enrolling residents as well as creating, administering and enforcing biometrics policies (UIDAI, 2010). The UIDAI prescribed guidelines on the biometrics technology, the various processes around enrolment, and verification procedures to be followed to enroll into the unique ID system. The UIDAI also designed and created an institutional microstructure, the Central ID Data Repository (CIDR) to effectively implement the biometrics policy, manage the central system, and created a network of registrars who will establish resident touch points through Enrolling Agencies.

The unique ID project saw people applying for an ID with the Enrolling Agencies that would go through some verification process and on approval by the Registrar; the applicant would be allocated a unique ID number. To apply for a unique ID number, applicants are required to submit data fields and biometrics, namely name, date of birth, father's/husband's/guardian's name and unique ID (optional for adults), mother's/wife's/guardian's name and unique ID (optional for adults), introducer's or a referee's name and unique ID, address and all ten finger prints, photograph and both iris scans (UIDAI, 2010). These details would be used to verify one's identity and avoid people from having more than one ID. Upon approval, the applicant is assigned a unique ID number; the UIDAI would forward the resident a letter which contains
his/her registered demographic and biometric details. The letter may also have a tear-away portion which has the unique ID number, name, photograph and a 2D barcode of the finger print minutiae digest (UAIDI, 2010).

For the unique ID project to succeed a number of initiatives were done. Among them, the project had the full support of the Indian government as a stakeholder, and different polices ranging from ethnic, cultural and technical issues were documented to guide the project (UIDAI, 2010, 2011; Zelazny, 2012). In addition, massive campaigns were conducted to create awareness and enhance social acceptance (UIDAI, 2010, 2011; Zelazny, 2012).

2.7 Overview of biometrics usage in Namibia

There is limited research on biometrics in Namibia. Much information is available on company websites and other online sources. One of the main sources of biometrics security information is from Mutelo's (2014) research work. The Biometric Research Laboratory (BRL) at Namibia Biometric Systems is the main organization that is deploying biometrics in Namibia. For instance, research by BRL in 2010 found that the deployment of biometrics driven Automated Teller Machines (ATMs) in banks which allow users to use their biometrics for verification and authentication are replacing cash card machines. Moreover, the biometrics solution can incorporate a suitable personal biometrics scanner to keep one's internet banking security firmly under their biometrics. The aim of the research by BRL was to replace the costly chip in bank cards with an individual's biometrics and eliminate the following limitations:

I. Card chip production - It costs banks a significant amount of money to pay for the chips used in the current bank cards. The cost of chip production is generally passed down to customers in various ways. Banks have to buy chips from chips manufacturing companies who also need to make a profit.

II. Bank Card Production - It is important for consumers to realize that banks also have to pay card manufacturers for the production of the banking cards who also need to make a profit. It is not a surprise that the cost is passed down to the clients in various forms.

In addition to banks, Automated Border Control (ABC) also uses the biometrics systems for automatically authenticating travelers at Border Crossing Points (BCPs) through the use of a passport reader.

2.7.1 Biometrics Implementation Challenges in Namibia

Mutelo (2014) noted that governments and commercial companies do not have in-house expertise and project management skills to manage or oversee the implementation of biometrics technology.

As a result, the project management team fails to identify sources of possible risks and measures to mitigate against such risks (Mutelo, 2014). This often leads to poor project management, risks the safe keep of data and the completion of the project. In some cases, vendors of the technology end up having a central role in the implementation of the technology without proper oversight (Mutelo, 2014).

2.8 Conclusion

The chapter discussed various biometrics traits that can be used for biometric security. It also outlined the implementation of biometrics as unimodal and multimodal biometrics. The chapter identified the necessary technologies required for deploying particular biometrics traits, among them image scanners and laser based scanners. It also outlined limitations of each biometrics trait such as damage due to manual work in the case of fingerprints, lack of body parts to use as biometrics traits in case of the disabled, and the use of contact lenses that may also affect the iris.

In addition, the chapter reviewed case studies in order to enhance the understanding of requirements for biometrics deployments. The reviewed case studies include India’s unique identification project that is widely considered in literature as a role model that developing countries can use to draw lessons on biometrics implementation. The reviewed case studies looked at measures that were taken to succeed with biometrics implementation. Among them included heavy government involvement or support, clearly drawn policies covering several aspects, engaged experts and monitoring teams to ensure that some unforeseeable challenges and other issues can be identified and addressed. The chapter also carried an overview of biometrics in Namibia, citing common areas where they are used and challenges faced.

CHAPTER 3: THE RESEARCH METHODOLOGY

The chapter articulates the research methodology and philosophical commitments. It also outlines the research design, data collection techniques used and respective data analysis techniques that were used.

3.0 Introduction

The previous chapters articulated the theoretical constructs of this research. This chapter contributes to this study by developing a research design guided by the reviewed literature to meet the research objectives. The research aims to design a multimodal biometrics framework for the Namibian government. Accordingly, this chapter adopts and explains its use of the research onion as proposed by Saunders, Lewis and Thornhill (2009) in identifying the core elements of the methodology, namely its philosophical commitments, research approach, and techniques for data collection and analysis.

3.1 Philosophical commitments

The Robert Wood Johnson Foundation (2008) views philosophy as beliefs that one assumes in the way the truth is extracted or the way a researcher extracts data from which the truth is derived. Morgan and Smircich (1980) (as cited in Collis and Hussey (2009) concede that the two main philosophies: positivism and interpretivisim are extreme philosophies on a continuum. Few people or researchers operate within these extremes of either philosophy (Collis & Hussey, 2009). However, "as one moves along the continuum, the features and assumptions of one paradigm are gradually relaxed and replaced by those of the other paradigm" (Morgan & Smircich, 1980 as cited in Collis & Hussey, 2009) as shown in Figure 4.

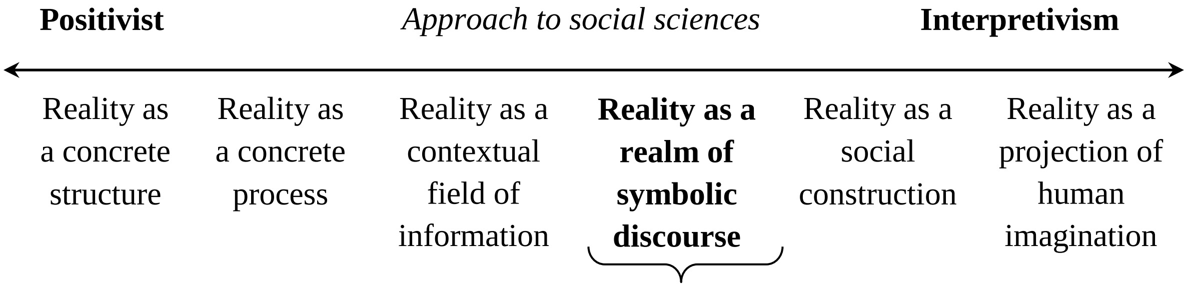

Positivist
Approach to social sciences
Interpretivism
Reality as a concrete structure
Reality as a concrete process
Reality as a contextual field of information
Reality as a realm of symbolic discourse
Reality as a social construction
Reality as a projection of human imagination

Figure 4: Continuum of core ontological assumptions (Morgan & Smircich, 1980 as cited in Collis & Hussey, 2009, p. 61)

Accordingly, this research leans towards the interprevism philosophy as shown in Figure 4. Interpretivism philosophy acknowledges that human beings are not mechanistic, and as such they have multiple realities which need to be understood within their context (Roux, 2005). Hence knowledge and meaning are acts of interpretation and there is no objective knowledge which is independent of thinking (Collis & Hussey, 2009). Interpretivism is often associated with qualitative research (Yin, 2003). However, due to the nature of the data to be extracted, this research also encompasses attributes of positivism.

3.2 Research approach

Saunders at al. (2009) concedes that there are two research approaches, namely the deductive and inductive approach. This research assumes the inductive research approach. The research started with the formulation of the statement of the problem and research questions guided by the literature. Its main aim is to design a multimodal biometrics framework for the Namibian government. The research is guided by the ICT roadmap methodological framework proposed by Jere et al. (2012). The idea is to demonstrate the implications of the economic, political and government, social and technological aspects in developing a reference document for multimodal biometrics deployment.

3.2.1 The ICT roadmap methodological framework

As indicated in the previous section, this research adopted the ICT roadmap methodological framework proposed by Jere et al. (2012) to meet the aims of the research: designing multimodal biometrics framework for the Namibian government. The ICT roadmap framework concedes that for any ICT stakeholder to offer a sustainable ICT solution in rural areas, economic aspects; political and governance aspects; technology aspects and social aspects have to be understood as shown in Figure 5 (Jere et al., 2012).

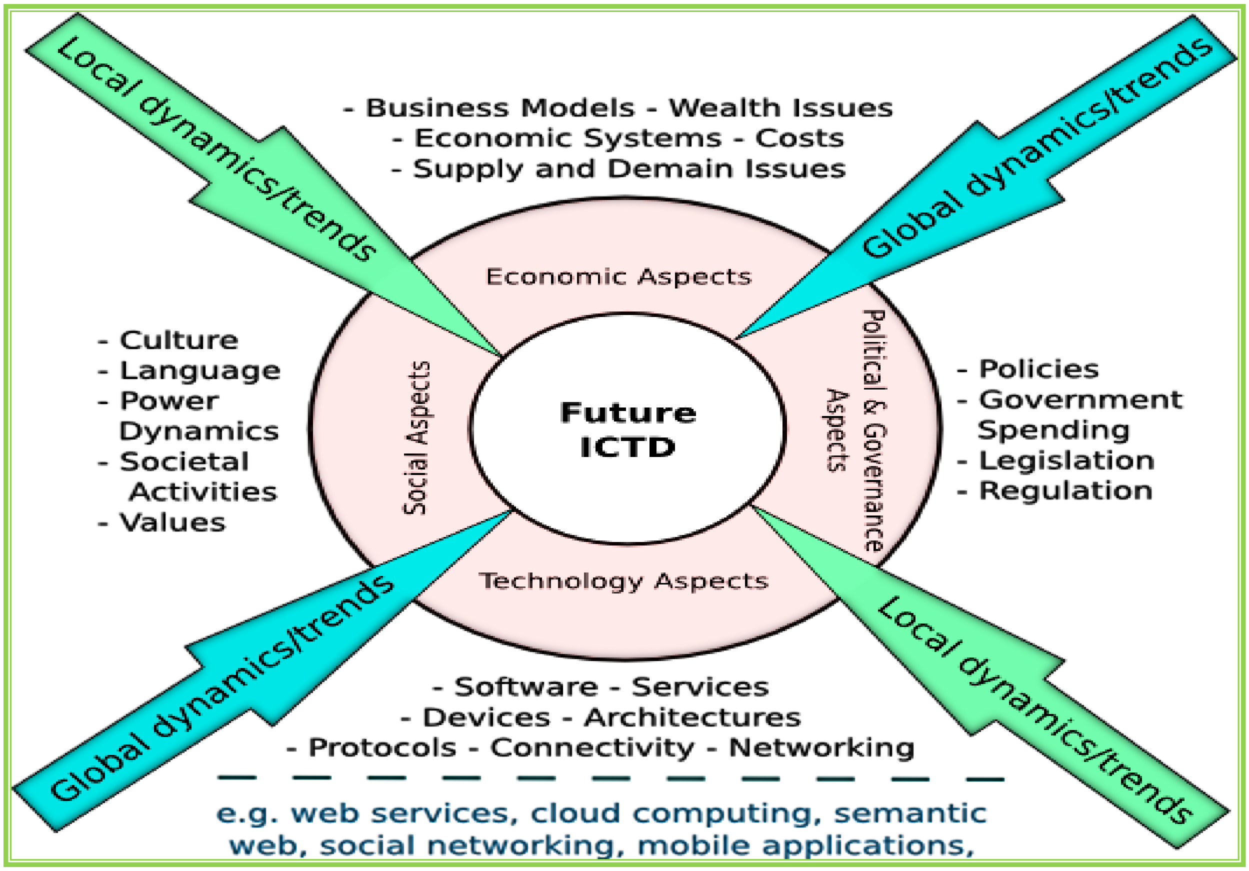


Figure 5: ICT roadmap methodological framework (Jere et al., 2012)

These aspects are partly influenced by local and global dynamics or trends. Each aspect is shaped or comprises of different critical factors; for instance the political and governance aspects consist of government policies, government spending, legislation and regulation. The economic aspect is determined by business models - wealth issues, costs, supply and demand. On the other hand, technology aspects focus on the software needed to support the ICTs, the infrastructures (devices, networking, protocols), while the social aspects include cultural issues, language, power dynamics, societal activities and values. It is believed that these elements play a critical role in depicting a country's direction in terms of its future ICT initiatives. In particular, the ICT roadmap methodological framework was developed partly based on propositions by Singh, Molla, Karanasios and Sargent (2008), which suggested that key characteristics and benefits of ICT initiatives have a strong impact on the economic, social, political and technical aspects. Kshetri's (2007) study agrees with these aspects by suggesting that the successful adoption and use of e-Commerce in developing Nepal (a developing country) is centred on economic, socio-political and cognitive factors. Economic and socio-political factors focus primarily on the environmental characteristics, while the cognitive component reflects organisational and individual behaviours (Kshetri, 2007). In this study, all these aspects are important and have to be understood before the implementation of multimodal biometrics.

3.3 Case study strategy

This research uses a case study strategy to answer the research questions and meet the research objectives. Creswell (1998, p. 61) as cited in Beverland and Lindgreen (2010) defines case studies as "an exploration of a "bounded system" [bounded by time and place] or a case (or multiple cases) over time through detailed, in-depth data collection, involving multiple sources of information rich in context". It is important to justify the use of the case study strategy to show its suitability to the study under consideration (Yin 2003). In particular to this study, the researcher has no control over the phenomenon understudy and the phenomenon cannot be studied outside the context in which it occurs. Additionally, the main research question: "*How should the Namibian government successfully prepare for multimodal biometrics deployment for different departments?*" includes a "how", which makes it suitable for a case study strategy according to Yin (2003).

3.3 The case study design

This section discusses activities and precautions that were considered through the use of the case study strategy. These include defining the unit of analysis, number of cases, case selection criteria, data collection techniques used and data analysis. These attributes are discussed next within the context of this research.

3.3.1 The unit of analysis

The unit of analysis relates to the case to be studied (Yin, 2003). Yin (2003) goes on to state that the unit of analysis is derived from key words that make the main research question of the study. Accordingly, the research question for this study is as stated below:

> "*How should the **Namibian government** successfully prepare for **multimodal biometrics** deployment for **different departments**?*"

Guided by the key words in the research’s main question above (shown in bold), this study’s unit of analysis shall be government departments that are already deploying biometrics securities. Chapter 2 articulated some of the Namibian government departments that are deploying or using multimodal and or unimodal biometrics securities.

3.3.2 The number of cases and case selection criteria

Even though single-case studies can richly describe the existence of a phenomenon, multiple-case studies typically provide strong evidence from multiple cases, which is often considered more compelling and the overall study is therefore regarded as being more robust (Herroitt and Firetone, 1983 as cited in Yin, 2003). As such this study uses multiple-cases for gathering the data to be used for meeting the research aims and answer research questions.

In addition, this research used the snowballing sampling method to select its cases for data collection. Snowballing sampling allows for cases with some experience of the phenomenon being studied to be selected. Just as laboratory experiments are not randomly sampled from a population of experiments, but rather chosen for the likelihood that they will offer theoretical insight, so too were the government departments that were selected for data collection in this research (Eisenhardt & Graebner, 2007). Accordingly, three Government Ministries namely the Ministry of Safety and Security, the Ministry of Home Affairs and the Ministry of Works and the Department of Roads Authority were selected as participants for this research.

3.3.3 Data collection instruments

The research made use of different data collection techniques to enhance the richness of the collected data. These techniques included a questionnaire, interviews, observations and document analysis. A case study protocol was used at every case during data collection for consistence purposes. A case study protocol contains the data collection instruments, procedures and general rules that were followed when using the data collection instruments (Dube & Pare, 2003). The use of the case study protocol is explained in each of the data collection techniques used in this study as outlined below:

- **Interviews -** interviews were used to collect data related to the political, governance and technology aspects as represented in the proposed framework for implementing the multimodal biometrics as shown in Figure 3. The interviews were based on predesigned structured questions that were guided by the attributes of the proposed framework for implementing multimodal biometrics. Only a single senior member within the IT Department or who is directly involved with biometrics was considered for interviews for each Government Ministry that was considered for this study. A full schedule of the interview questions is provided in Appendix A. Below is an outline of the interview questions, what they assessed and how they relate to the political, governance and technology aspects of the proposed framework for implementing multimodal biometrics:
    - **Political and governance aspects**:
        - Polices ➔ Assessed through interview question 1, 5
        - Government spending ➔ Assessed through interview question 7
        - Legislation ➔ Assessed through interview question 1
        - Regulation ➔ Assessed through interview question 5
        - Stakeholders ➔ Assessed through interview question 6
    - **Technology aspects:**
        - IT infrastructure ➔Assessed through interview question 2
        - Biometric technologies in use ➔Assessed through interview question 3
        - Biometrics challenges ➔Assessed through interview question 4
        - Biometric necessity ➔Assessed through interview question 8
        - Viable maintenance policy ➔Assessed through interview question 9
- **Questionnaire -** a questionnaire was also used for data collection. Five to ten respondents were selected from each ministry to complete the questionnaire. Between five and ten respondents were considered per ministry as most ministries have a small IT staff complement. The researcher had inside information in terms of the IT staff compliment as he is a senior member in one of the Government Ministry. Participants were selected using a simple random selection probabilistic sampling method. Names of the targeted population were written on small pieces of paper, put in a box and randomly picked, with the picker blind folded. The questionnaires were used to collect data for evaluating the proposed framework for implementing multimodal biometrics. In particular, the questionnaires were used to provide additional supporting

evidence (to data collected through interviews) from junior staff members. A full schedule of the questionnaire is provided in Appendix B. The questionnaire is divided into two sections. The first section (question 1 to 6 - open and some closed ended questions) collected data for evaluating one's knowledge of biometrics. This relates to the data on what biometrics does the respondent know, the biometrics they have used, biometrics they prefer to use and challenges they are facing in relation to biometrics implementation within their ministry. In particular, question 6 is open ended and collected data on challenges of biometrics that shall be aligned to the different aspects in the proposed framework for implementing multimodal biometrics during evaluation.

In addition, the second section of the questionnaire is based on a 5 point Likert scale that is categorized as follows: 1 - strongly disagree, 2 - Disagree, 3 - Neutral, 4 - Agree and 5 - Strongly Agree. This section has 22 questions that collected data relating to the challenges associated with biometrics during deployment and usage. These challenges align to the political, governance, economic and technology aspects in the proposed framework for implementing multimodal biometrics as outlined below:

  - **Political and governance aspect -** assessed using data collected by question 16 to 21
  - **Economic aspect -** assessed using data collected by question 8 and 9.
  - **Technology aspect -** assessed using data collected by question 1 to 7, 11 to 15 and 22. As noted in previous studies evaluating economic, political and technical factors of technology adoption and use, the technical aspect often contributes a lot of challenges in developing countries (Kshetri, 2007).

- **Observations** - were used to collect data for supporting thick descriptions on data collected through interviews and questionnaires (Dube & Pare, 2003). Observations were aimed at collecting data on how biometrics are deployed and used at every ministry considered for data collection. In addition, observations were used to collect data on one's facial expressions during interviews.
- **Document analysis -** document analysis was conducted on existing documents, namely policy documents, ministerial websites, network deployment diagram and emails. The aim was to collect data for supporting thick descriptions.

3.3.4 Ethical consideration

In relation to the case study protocol for this research, an ethical clearance was sought from the Polytechnic of Namibia, Informatics Department prior to data collection. Participants were asked to sign an informed consent form prior to participating in the survey. The informed consent specified the aims of the research and expressed that all the data collected was going to be used for research purposes only and researcher was going to keep the identity of the participants anonymous and confidential. A copy of the informed consent is attached in Appendix C. In addition, the identity of ministries and respective interviewees who participated in this research' data collection was kept anonymous. Ministries were labelled (for instance Ministry A) and no mention of their identity was made. This is common practice to ensure that the identity of participants is kept confidential as was also done in studies by Beverland, Ewing and Matanda (2006) and Irani, Alshawi and Missi (2011).

3.3.5 Data analysis

The data collected through interviews, observations, questionnaire and document analysis were analysed together as these approaches were adopted during data collection with the aim of supporting thick descriptions as proposed by Dube and Pare (2003). Data analysis from each participant was done separately, identifying relevant information and then collectively analysing it together, identifying matching and unique emerging themes. The following steps were followed during data analysis:

3.3.5.1 Within case analysis

Within case analysis involves the analysis of data for each ministry considered separately. The aim is to establish views of participants from each ministry. The following steps were followed during the within case analysis:

1) **Transcribing of tape recorded data** - considering that interviews were tape recorded, data analysis for interviews started with the transcribing of the recorded data to obtain a full record of the conversation. Transcribing was done for each participant or case (ministry) separately.

2) **Coding of data** - considering that interviews were based on structured questions, all responses for each question were analyzed within the respective question. Data was analyzed within the aspects of the ICT roadmap theoretical framework, considering that questions in the questionnaire and interviews were designed to address aspects of the theoretical framework. These included the economic, political and governance, technology and social aspects. Any emerging themes were identified, given a title or thematic name that describes them. In addition, data collected through the Likert scale based on the questionnaire for evaluating the deployment and use of biometrics was analyzed using the view of the majority participants for each case considered. Data collected through the questionnaire was analyzed using excel, except question 6. Question 6 of the questionnaire was used to establish emerging themes through data collection and as such, any emerging themes from question 6 were given their own category. In some cases, data from question 6 of the questionnaire was used to support findings from other data collection techniques. Supporting data collected through document analysis and observations were also included to add weight to the research findings from the interviews.

3.3.5.2 Cross-case analysis.

Once all data for each case was separately analysed, cross-case analysis began. Cross-case analysis was conducted, identifying matching and contrasting responses from participants. The aim of the cross-case analysis was to ensure that findings from data collection are better grounded and are well informed. Information from the cross-case analysis was used for designing multimodal biometrics framework for the Namibian government.

3.4 Conclusion

This chapter discussed components of the research methodology for this research that were used to meet the objectives of the study and address the research question. In particular, the research explored its philosophical commitment which is aligned to the interpretivisim philosophy. In addition, the research followed an inductive approach guided by the ICT roadmap methodological framework. The research used a case study strategy within the interpretivism philosophy. The chapter also outlined the case study design, and identified its unit of the analysis - ministries of the Namibian government that adopted multimodal biometrics. As part of the case study design, the research specified on the number of cases and the case selection criteria used during data collection. Three cases were considered for this study and snow balling was used for selecting cases. In addition, the chapter outlined the data collection instruments, which included the use of interviews, document analysis, observations and a questionnaire. The chapter also discussed its commitment to ethical considerations.

The next chapter presents the data collected using the research methodology explained in this chapter.

CHAPTER 4: TOWARDS A FRAMEWORK FOR IMPLEMENTING MULTIMODAL BIOMETRICS TECHNOLOGY: PRESENTATION OF FINDINGS

This chapter presents the findings from each ministry separately considered during data collection.

4.0 Introduction

This chapter presents the findings from the data collected across the different ministries. Data collection was done according to the methodology as specified in chapter 3. The collected data focuses on the implementation of multimodal biometrics technologies in the Namibian government departments and or ministries. As such, the data is used to meet the aim of this thesis of designing multimodal biometrics framework for the Namibian government.

In particular, this chapter presents results from each ministry considered during data collection. The aim is to present the views of participants from each ministry in relation to their experiences from the implementation of multimodal biometrics technologies. Data analysis is limited to data gathered through interviews and the questionnaire. Only questions one to six of the questionnaire are used to assist and support arguments raised through the interviews. It should be noted that the research methodology for this thesis was developed as guided by the ICT roadmap theoretical framework proposed by Jere et al. (2012). As such, the data analysis of this chapter presents research findings according to different aspects or dimensions that make up the ICT roadmap theoretical framework. The focus is on the assessed aspects.

4.1 Ministry A - an overview

Ministry A has a custodial domain over two departments, both responsible for different aspects of national safety and security. Ministry A and its departments were established by the Act of Parliament with the functions articulated in the Act, and are summarised as follows:

Preservation of the National Namibian security through the maintenance of law and order, the protection of life and property and general investigation and prevention of crime.

The head of Department A (one of the two departments under the ministry A) is an appointee of the President of the Republic of Namibia in terms of the Namibian Constitution. Department A comprises of staff appointed by the Department’s heard in accordance with the Act. Amongst the numerous departments within Department A, this thesis specifically concentrates on the

Communications Directorate. The directorate's mandate is that of managing Information, Communications and Technology on behalf of Department A. Most recently the directorate has embarked on a project aimed at digitalizing operational aspects of policing. These systems are:

- The Electronic Policing system
- Automated Biometric Identification System
- Security for buildings and/or facilities

Collectively, these systems will modernise operations and introduce efficiencies, while not placing any more strain on limited and over-taxed human resources. More specifically:

1. Decisions in most modern operations are information driven. This is one of the reasons for the success or failure of the introduction of technology in an environment with the primary purpose of automating previously manual operations.
2. Most secure facilities are designed and built for a single purpose. This limits their useful life span and makes them ill-suited to changing environments. This premise applies for facilities meant to house criminals. Department A's stations have evolved from facilities for temporary incarceration and processing for the aforementioned purpose. Thus it is required to introduce multi-facetted security systems which can allow for old stations to be "upgraded" with minimal disruptions to on-going operations and additional strains on capital, both human and monetary.

Ministry A is currently implementing its multimodal biometrics, a process that started in 2015. Ministry A has an IT staff complement of 30 members. A total of five questionnaires were issued to respondents within Ministry A and only four questionnaires were completed despite a relatively big staff complement, leaving one questionnaire uncompleted. This could be attributed to the fact that multimodal biometrics technologies are still new to most employees of this ministry, considering the fact that data collection was done towards mid-year, barely six months after the commissioning of multimodal biometrics in Ministry A.

4.1.1 Findings on Ministry A's implementation of multimodal biometrics technologies

Considering that Ministry A has two different departments (with their own ICT divisions and heads) mandated with critical roles by the Namibian government, it was decided to interview two senior members from Ministry A - one senior interviewee per department. Findings from the interviewees were analysed together with those of the questionnaire focusing on question one to six. Data is analysed within the confines of the ICT roadmap theoretical framework's different aspects as specified in chapter 3, section 3.3.5.1. These aspects or dimensions include the technological, political and governance, economic and social aspects.

4.1.1.1 The technology aspects

Data was gathered to evaluate factors surrounding the technological aspect in relation to multimodal biometrics deployment and usage. The gathered data relates to biometrics use, IT infrastructure, biometrics technologies in use, biometrics challenges, the need for biometrics and the need for a viable maintenance policy.

1. ***Biometrics use***

Data collected through the questionnaires shows that all IT employees engaged in data collection have the knowledge of multimodal biometrics. When asked to indicate if participants have knowledge of a set of biometrics traits, participants indicated that they know at least two biometrics traits as shown in Figure 6. The fingerprint is the most (4) common biometrics trait, while the hand geometry and signature are the least known (2). This could be attributed to the fact that Ministry A uses fingerprints, face and iris among other biometrics traits for controlling physical access to its premises (CPA), for accessing personal devices (APD), for accessing personal information (API) and the verification of information (VoI). One of the interviewees admitted to using fingerprints and other biometrics by stating that: "*we use finger prints intensively, we open doors with finger prints, we start instruments with fingerprints, now you can imagine when we do certain forms of analysis and you don't want to use a fingerprint*". The interviewee went on to explain that in some circumstances, it is impossible to use fingerprints as such and other biometrics traits come into play. The interviewee explained that : "*…you don't want to touch equipment while you are in analysis with your fingerprint and you can't because you are normally gloved up and you can't activate such a reader with that (fingerprint), so we resort to iris technology and in certain instances we resort to voice so we use them all as we go along.*" In addition, the interviewee also highlighted that they have equipment that uses ear and face geometry for human identification. The interviewee explained that: *"when we talk about human identification in some cases,* *fortunately not the majority because its time consuming, we resort to biometrics principles with which we can then identify, such as ear geometry, facial geometry."*

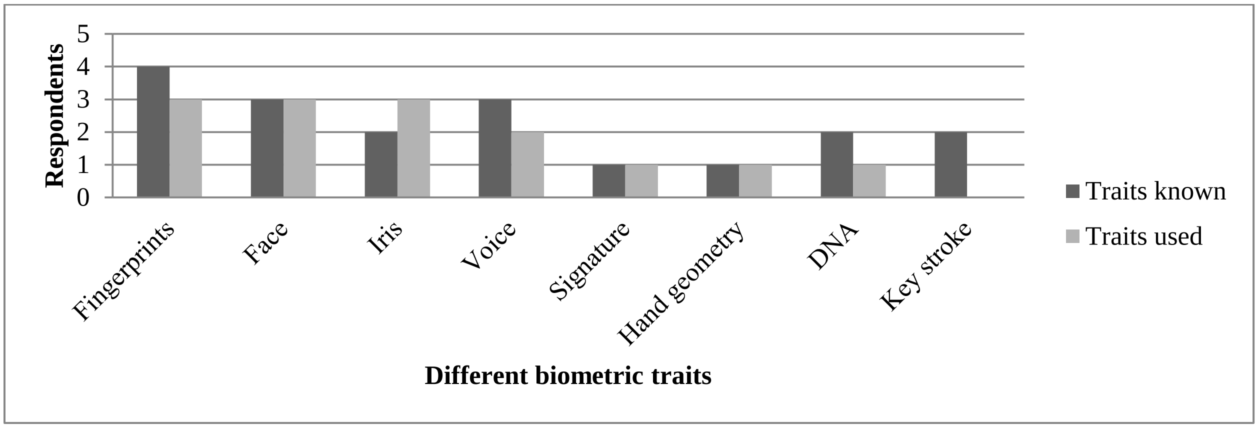


Figure 6: Used and known biometric traits

The second interviewee from the other department under Ministry A also confirmed the use of multimodal biometrics by stating that: "*So biometrics is an important technology for <department name provided> because it enhances security by controlling access to information as well as providing accurate identification of offenders throughout their lifetime."*

2. *Biometrics necessity*

Data related to the need of multimodal biometrics was collected. The aim was to see if users see the need of biometrics through the roles it plays within the whole system. As such participants were asked if they feel there is a need for biometrics. One participant respondent: *"Absolutely, I am 100% behind them (use of biometrics), there is no story about it. As the human population increases and as demand for identification increases, referencing increases, you will not be able to provide a service, which ever service, without this technology."* The interviewee went on to stress that the choices of biometrics depends on the circumstances or working environment: *"Which one I prefer most - I think horses for courses - that means for each type of application one will need something that is unique with various advantages but also various disadvantages so one will have to select what is very unique to that environment."* As highlighted in the section above, a combination of fingerprints and iris appear to suit this ministry well.

3. *Biometrics challenges*

Interview questions and question six in the questionnaire gathered data relating to multimodal biometrics challenges. Different challenges were identified ranging from technical challenges, preparing staff on biometrics, economic challenges, acceptance of the use of biometrics and legal challenges.

- Technical challenges - data collected through the questionnaire shows that the slow network negatively affects the effectiveness of biometrics. On the other hand, biometrics are difficult to work with when operating in a decentralized network, with centres not networked together. One interviewee stated that: *"We want to have a centralized access point for the biometrics and until such wide area network is created, we find it hard to implement (biometrics)"*. In addition, two respondents cited challenges associated with fingerprint based biometrics systems namely; the failure to match fingerprints of existing users due to normal malfunctioning, forcing users to do many trials, at times the system fails to read fingerprints of the old people and or physical labourers. In addition, having to carry access cards is also seen as a challenge and the system is often down when offline. Lastly, one interviewee lamented that biometrics technologies involve different technologies with different product life cycles that bring in compatibility challenges.
- Preparing staff on biometrics - one interviewee noted that quite often the focus is on *"the nuts and bolts but we forget things like the biometrics systems"*. Thus, focus is always on the biometrics but little effort is made in equipping the staff (old and new staff members) with the skills on how they can work with biometrics.
- Economic challenges - both interviewees and participants who completed the questionnaire noted that biometrics technologies come at a high cost when buying for the first time as well as maintenance.
- Acceptance and use of biometrics - one interviewee noted that *"you find that people are quite apprehensive, they feel it's needless or too much extra trouble so it's also very important that you also get a buy in from your human resource"* to avoid sabotage or a denial of system use. The interviewee noted that quite often users deactivate system alarms, or *"put a brick in a door"* because they do not quite understand the need for it. *"The good way to go is to sensitize them about change; that these things have come to stay, they will not go back again and we need to make them aware of that."*

- Legal challenge - common legal challenges come as the staff does not want to have their biometrics traits profiled or other important government departments are yet to use biometrics technology. This is common in organisations that use biometrics systems as they request for users' specific biometrics trait profiles. One interviewee from Ministry A stated that quite often people say *"I only applied for the job I never gave permission that my DNA be profiled".*

4. *IT infrastructure*

Interview questions collected data for evaluating participants' view on IT infrastructure in relation to biometrics implementation. One interviewee from Ministry A stated that their implementation of biometrics technology is currently going through phases of laying out the IT infrastructure as well as biometrics specific technologies: *"Currently the NCS is facing great emphasis on deploying networks and server infrastructure across all its regions or technologies such as biometrics to be able to be used effectively, so currently we are busy setting up foundations to be able to use such services (biometrics)"*

5. *The need for biometrics*

Both interviewed senior members in the IT departments supported the need of biometrics, considering the nature of work their Ministry is mandated to do. One interview explained: *"Biometrics are crucial to control access to information, access to restricted areas, as well as identifying offenders when they are in incarceration because they come with different names."* In addition, the second interviewee also indicated that he is "*absolutely100% behind them*" referring to the use of biometrics. The second interviewee went on to explain the importance of biometrics in line with his nature of work by saying that *"as the human population increases and as demand for identification increases, referencing increases, you will not be able to provide a service, which ever service, without this technology."*

6. *Availability of a maintenance policy*

In relation to the maintenance policy, one interviewee indicated that the presence of a maintenance policy is crucial for the implementation and use of biometrics. Even though Ministry A is already implementing the biometrics technology, the maintenance policy is yet to be finalised. One interviewee indicated that *"we are in the process of establishing and approving various polices* *and the maintenance policy is part of this process. When it's specific to biometrics we have not fully implemented it as yet, we are still looking into adding this aspect or feature into the policy as the time goes."* In addition, the second interviewee highlighted the need for a maintenance policy to ensure the "*routine maintenance*" of hardware, software, policies and administration in order to "*avoid reflex reaction, where you react when it's too late*". The interviewee went on to state that these maintenance procedures *"... cannot be routine enough, rather they should always be more frequently"* to avoid system failure in a complicated IT environment. These maintenance procedures should be in place to complement the already existing inbuilt system check-ups.

4.1.1.2 The political and governance aspect

Questions relating to this aspect collected data to evaluate issues related to biometrics policies and stakeholders.

1. ***Policies***

The aim of questions under this segment was to collect data that would evaluate the presence, need and use of biometrics policies and plans. Research findings show that both interviewees under Ministry A agree on the need of polices with regards to the implementation and use of biometrics. One interviewee stressed that *"there has to be a policy in place, the policy should outline the usage of biometrics and the storage of data and privacy concerns because we are talking about using the fingerprints of members as well as offenders."* However, one of the two departments under Ministry A does not have a policy on biometrics as the interviewee stated that *"Yes it's* (referring to the biometrics policy) *not in the place yet",* when asked about the presence of a biometrics policy or plan. What is currently in place is the IT strategic plan and it appears biometrics are treated or seen as part of IT. The interviewee explained how the IT strategic plan supports biometrics deployments: *"Basically our IT strategic plan focusses on creating an enabling environment for our members as well as finding technological solutions within our Department. The goal is reached through three strategic pillars namely infrastructure, security and information sharing, so biometrics is an important technology for our department because it enhances security by controlling access to information as well as providing accurate identification of offenders throughout their lifetime."* Even though they do not have a stand-alone policy or implementation plan for biometrics, the interviewee explained the steps they are following to implement their biometrics, which involves coming up with the implementation strategy that specifies how to implement, test and roll out biometrics. The interviewee explained how they are implementing their biometrics: *"we started with the Head Office where we are testing the system; this will follow further implementation strategy."*

Nevertheless, the second interviewee from a different department under Ministry A confirmed the presence of polices and plans on biometrics. The interviewee explained: *"we have got various schemes and polices and plans that are well strategized with forward looking and are planned well in advance".* The interviewee explained the factors that determine how they roll out their biometrics starting with the sourcing of funding: *"what we do is we roll them out with the necessary interventions of the Medium Term Economic Framework cycles, the budgetary cycles. So we roll them out as directed by these cycles and as we expand so we look at scalability, issues of funds and issues of need and these are some of the factors that drive the roll out."*

2. Stakeholders

Questions under this subject looked at collecting data for identifying stakeholders involved in biometrics and their roles. One of the interviewees identified their stakeholders as those involved in the acquisition, enrolling of biometrics technology and "*those involved with the permanent storage and maintenance of it*". The interviewee further highlighted the presence and role of the government as a stakeholder to whom they make applications (on any proposed IT plans) to for approval and be granted permission, which is a process that involves consulting a number of *"government bodies"* something that is seen as a frustrating impediment in the eyes of *"project teams who want to roll out the technology"*. Nevertheless, the interviewee acknowledges the government's support towards IT plans: "*IT plan is one of our government polices if we look at our long term development plans and projects (*one could see) *that ICT and IT planning is a fundamental part there"*

The second interviewee identified the IT Department as the *"Directorate for Security* - *which is spearheading the biometrics implementation"* and the government as the key stakeholder. The interviewee further highlighted that the government as a stakeholder, *"understands the need for more accurate identification"* and as such *"embarking on such a project* (referring to IT plans) *is not something that is really denied by government."*

4.1.2 Summary of Ministry A Findings

The table below summarizes findings from Ministry A within the aspects of technology and government.

Table 3: A summary of findings from Ministry A.

Technology Aspect	**Biometric traits in use:**	− Fingerprints − Face − Iris − Voice − Signature − Hand geometry − DNA
	Need for biometrics	− They see the need
	Biometric challenges	*Technological challenges:* − A viable computer network − False rejection of registered users as the system fails to capture and match prints. − Failure to detect some finger prints of the old and manual labourers − Compatibility issues *Economic challenges* − Costs *Other challenges:* − Lack of training − Technology acceptance − Legal challenges
	IT infrastructure	− Laying out computer network
	Maintenance policy	Not available
The political and governance aspect	**Policies**	− Recognise the need for government policies for biometrics − Have an IT strategy
	Stakeholders	− government as major stakeholder

4.2 Ministry B - an overview

The primary objectives of Ministry B are to manage and administer the national population register, facilitate lawful migration and to receive and protect refugees and asylum seekers. Ministry B aims to ensure that every Namibian citizen is able to obtain national documents in a simpler, faster and convenient manner. The ministry has two departments that fall under it. For anonymity reasons, the departments are herein referred to as Department A and Department B and their duties are outlined below:

4.2.1 Department A's duties and responsibilities:

- Registration of births and issuing of birth certificates
- Registration of death and issuing of death certificates
- Issuance of duplicates of birth certificates.
- Processing applications for alterations, re-registration and change of surname
- Receive Identification Document (ID) applications, register and classify the finger prints on the ID application form, capture the demographic data provided on the form, scan imported images, thumb prints and signatures, check listing, verification and approval of application, produce and dispatch identity documents.

4.2.2 Department B's duties and responsibilities:

- Grant and issue Namibian passports and emergency travel certificates
- Grant and issue citizenship to foreign nationals
- Grant and issue various permits to foreign nationals
- Grant and issue various visas to foreign nationals
- To issue domicile certificates to foreign spouses of Namibian citizens
- The effective facilitation of lawful migration

The Information Technology Division under Ministry B is responsible for the implementation, support or management of computer-based information systems within the ministry.

4.2.3 Findings on Ministry B's implementation of multimodal biometrics technologies

The following section outlines the findings from Ministry B, grouped according to different aspects of the theory that was used as a source of guidance during data collection. Only one interviewee was engaged because Ministry B has only one IT department that oversees all departments under Ministry B. The Head of IT in Ministry A participated in this research's interviews during data collection.

4.2.3.1 The technology aspect

The conducted interviews focused on collecting data relating to the IT infrastructure, biometrics technologies in use, biometrics challenges, biometrics necessity and the presence of a viable maintenance policy. The following findings were made in relation to the technology aspect:

1. *IT infrastructure*

The interviewee confirmed the presence of a viable IT infrastructure in place. The interviewee explained: *"Yes there is supporting infrastructure available, currently we have signed a service labour agreement with the vendor of the system."* Such infrastructure includes biometrics specific equipment like fingerprints detectors. In particular, Ministry B has implemented an Automatic Finger Print Integrated System (AFIS) that allows for information verification through the use of one's fingerprints. In addition, networked servers are also available that store data. In particular to servers, departments in Ministry B have a primary server and a secondary server to take over service provision in the event that the primary server is down or malfunctioning.

2. *Biometric technologies in use*

The most common biometrics technologies used at Ministry B are fingerprint based systems. All participants who completed a questionnaire indicated that they use fingerprints as a biometric trait and as such, they have fingerprints detectors or captures. In support of this, the interviewee confirmed the use of fingerprints by stating that they have implemented the fingerprints system called AFIS. AFIS is used for ID generation with its attributes of information verification, making sure that *"each and every national is issued with one ID even if they change their name."* In addition, the interviewee indicated that fingerprints are also used to control access of various areas in the building.

In terms of future plans, Ministry B is looking into capturing fingerprints in the passport to replace the bar code reader machine that is currently in use, as they move towards tightening their system through biometrics and plugging all possible loop holes. In addition to this, currently in place is the face recognition system that is being done manually as the staff compares the face in the passport or ID against the holder. Plans are underway to engage biometrics technologies that use face recognition through the use of a chip to be carried around that will carry one's image, fingerprints and demographic information. The interviewee explained how it will work: *"Then whenever you swap you indicate your passport to our readers, it will compare your face with that on the chip that is already a facial recognition."*

3. *Biometrics challenges*

In relation to challenges, the interviewee identified the availability of funds to bankroll biometrics purchase and implementations as one of the major challenges. This is mainly so because technologies change every now and again. The interviewee explained: *"The challenge that we are facing is financial, these are new technologies and technologies change every 4th year or 5th year and you have new equipment to be replaced and so forth and that requires a high budget to keep pace with the changing technologies".* The issue of funds to bankroll biometrics projects was highlighted twice by the interviewee, something that emphasised the magnitude of the challenge.

The interviewee further highlighted that network connectivity used to be one of the problems, in particular to "*remote areas*" but now it's *"a thing of the past because our country is covered 90% with fiber optic".* Despite this, there are other notable challenges which are as follows:

- System often goes offline
- Regular maintenance as the system malfunction due to user miss-use.
- False rejection of registered users as the system fails to capture and match prints.
- Failure to detect prints especially when one's fingerprints are damaged
- Not suitable for those with no hands
- Fingerprints images on the ID card often get omitted resulting in the system failing to get accurate prints.

4. *Biometrics necessity*

When asked on the needy for biometrics, the interviewee mentioned that the use of biometrics especially within Ministry B involves the identification of nationals. The interviewee saw biometrics as a way to *"curb fogginess and also verification purposes."* The interviewee explained: *"Since our institution is mandated to identify a person even if you change your name or details, we must have a mechanism of identifying that you are the right person you claim to be. Biometrics is one of the technologies that one can use and rely on."* The interviewee further highlighted the need for adding more biometrics traits to complement fingerprints, with the face or iris seen as the best option in order to improve the quality of their verification systems.

5. ***Viable maintenance policy***

The interviewee confirmed the presence of a maintenance policy for individual systems used by Ministry B's departments. Such systems include the passport system for issuing passports, ID issuing system, border control management system, AFIS and citizenship issuing system. These systems have a *"maintenance plan where routine checks are done and also troubleshooting depending on the performance of the system."* According to the interviewee focus will be on both hardware and software components of the system. As indicated by one participant who completed a questionnaire from Ministry B, these biometrics technologies require *"regular maintenance due to malfunctioning or miss-use by users"*, something that indicates that maintenance is often done on demand, that is when there is faulty equipment.

4.2.3.2 Political and governance aspects

Findings on the political and governance aspects which include policies and stakeholders are outlined below:

1. ***Policies***

In particular to polices, data was gathered to evaluate how Ministry B's IT plan or policy supports the implementation of biometrics. In relation to this, the interviewee from Ministry B indicated that they have an IT plan at ministerial level, not departmental level:*"Yes we have a (IT) plan in place"*. The IT plan is the one guiding Ministry B with the incorporation of AFIS (within their IT systems), a system they use for issuing national identity documents. The IT plan ensures that Ministry B is *"issuing documents to the rightful people, verified information"*. As such, Ministry B's IT plan supports the deployment of biometrics in the sense that biometrics, through the use of fingerprints are used as a *"means to verify and register nationals."* "*Even if they change (nationals) their names we can verify with fingerprints, which cannot change*" something that avoids individuals from having more than one ID or "*duplicates*".

However, when it comes to having an official policy or plan on "the step by step" implementation of biometrics, the interviewee from Ministry B highlighted that they don't have such a plan. Instead, the interviewee stressed that the need to implement biometrics is necessitated or driven by *"demands and relations from other institutions"* using such biometrics. For instance, institutions like banks and insurance companies are pushing for the use of fingerprints based verification systems and as such, Ministry B as the country's official ID issuer has to incorporate fingerprints in nationals' identification documents.

2. Stakeholders

Data relating to stakeholders and their roles was collected. It was found that Ministry B's stakeholders include the office of the Prime Minister, *"who authorize the implementation of our systems",* the Police department which identifies criminals, immigration officers, and the Forensic Institute, which are *"connected to* (Ministry name provided) *to make sure that they also use the system when doing investigations."*

When asked about the support on IT plans that the Ministry B gets from the government as a stakeholder, the interviewee indicated that they do not get much support. The interviewee explained how they manage their biometrics: *"Not as such* (in reference to getting support from the government)*, they don't go in detail on advising us how to do it; we get demands from institutions, JBF, Banking institutions and insurance companies, that's where we get our plan on how to implement it to answer to their problems and also the internal directorates that are issuing national documents. Based on their demands we plan on that but we don't get financial support from them, they come requesting for a service only. "*

Even though the interviewee did not specifically identify institutions in the commercial sector such as banks and insurance companies as stakeholders, based on the empirical evidence, it can be argued that these institutions are also stakeholders of Ministry B. This is so because these institutions initiate or in a way suggest what biometrics technology Ministry B should consider and implement.

4.2.4. Summary of findings from Ministry B

Table 4 below shows a consolidated summary of findings from Ministry B.

Table 4: Summary of findings from Ministry B

Technology Aspect	**Biometric traits in use:**	− Fingerprints − Face
	Biometrics need	− Realise the need. Seen as a solution to forgery
	Biometric technologies in use	− AFIS

	Biometric challenges	*Technological challenges:* − Regular maintenance as the system malfunction due to user miss-use. − High false rejection of registered users. − Failure to detect prints especially when one's fingerprints are damaged − Fingerprints images on the ID card often get omitted resulting in the system failing to get accurate prints. *Economic:* − Costs − Availability of funds *Other challenges:* − Not suitable for those with no hands
	IT infrastructure	− Have a viable computer network
	Maintenance policy	− Have a maintenance policy
The political and governance aspect	**Policies**	− Have an IT strategy
	Stakeholders	− Government-limited support in terms of advice on biometric uses − Police Department

4.3 Ministry C - an overview

Ministry C's mandate is to manage Namibia's national road network with a view to achieve a safe and efficient road sector. The management of the proclaimed road network includes planning, designing, construction and maintenance.

In addition to its core functions, Ministry C also provides the following services to vehicle owners, operators and drivers as assigned functions from the Ministry of Works and Transport in terms of Section 111 of the Road Traffic and Transport Act, 1999 (Act 22 of 1999):

- Vehicle registration, licensing and roadworthy testing
- Driver testing and licensing
- Vehicles Registering Authorities

- Regulate National (domestic) and Cross Border Road Transportation

4.3.1 ICT in Ministry C

One of Ministry C's main strategic initiatives is that of digitalizing and streamlining business processes. As such, Ministry C has an ICT department whose role is to plan, design, implement, administer and manage all ICT aspects. Ministry C has a number of critical national ICT systems such as:

- National Traffic Information System (eNaTIS) - This is a register of all road traffic and users in the country. It is the core system to Ministry C and is used at all registering authorities across the country as well as by a number of third parties such as Nampol, BoN, CoW and RFA.
- Cross Border Road Transport System (CBRTS) - This system deals with the issuing of permits to the Namibian road traffic crossing Namibian borders into neighboring countries.
- Road Transport Permit Module (RPTM) system - This system provides permits authorizing the transportation of passengers for a fee, travelling on public roads within the borders of Namibia.
- Abnormal Load Permit System (ALPS) - This system provides for exemption permits authorizing the transportation of abnormal loads and/or movement of abnormal vehicles travelling on public roads within the borders of Namibia.
- Traffic Management System (TRAFFMAN) - This system has a weighbridge module and is thus used at all national road weighbridges. Its function is overload control with a view to protect national roads from damage emanating from overload.
- Road Management System (RMS) - This is a repository system containing all relevant information pertaining to all national roads. The system contains information such as road conditions, traffic count, materials used, age, and maintenance frequency. This system is critical in gathering information for planning of the road network.

In addition to the above mentioned national systems, the authority also has an enterprise resource planning system. This system integrates, digitalizes and modernises the following business processes:

- Human Resources administration
- Payroll
- Finance and budgeting
- Project Management
- Procurement
- Asset Management

This system caters for a smoother administration of support functions, which enables the authority to optimally carry out its core functions in achieving its mandate.

4.3.2 Findings on Ministry C's implementation of multimodal biometrics technologies

Only one interviewee was engaged because Ministry C has only one IT department that oversees all Departments and or Divisions under Ministry C. The Manager of Analysis and Applications for ICT at Ministry C participated in this research's interviews during data collection. In addition, Ministry C has a staff complement of sixteen members in their IT Department and biometrics has been in use at Ministry C for approximately ten years. Below is an outlay of findings at Ministry C, grouped according to different aspects of the theory that was used as guidance for data collection. These findings are limited to data collected through the interviews supported by question 1 to 6 of the questionnaire. Given that Ministry C has a relatively big IT staff complement with more years of biometrics use, it was decided to engage nine respondents for the questionnaire. One questionnaire was spoiled and eliminated from those that were analysed.

4.3.2.1 The technology aspect

The conducted interviews focused on collecting data relating to the IT infrastructure, biometric technologies in use, biometrics challenges, biometrics necessity and the presence of a viable maintenance policy. The following findings were made in relation to the technology aspect:

1. ***IT infrastructure***

The aim of this attribute was to gather data for evaluating the presence of IT infrastructure that support biometrics. Data collected at Ministry C shows that the ministry has IT infrastructure to support biometrics ranging from hardware to software elements. Thus, all their ICT systems are supported by a state-of-the-art ICT infrastructure comprising of servers, storage and network spanning across the country. In particular to hardware elements, the interviewee identified fingerprint scanners, servers for storing images of fingerprints and hard drives for transporting images. Software in use includes *"the finger print image software and the finger print matching software".* Ministry C has approximately 87 sites countrywide which are interconnected by a Multiprotocol Label Switching (MPLS) technology in forming one network for efficient and effective communication and resources sharing. Ministry C manages its bandwidth for scalability purposes. Through the MPLS, Ministry C has a network tool that can split the bandwidth into slots *"to give certain traffics a preference."* In addition, the transfer of biometrics images is done at night when business is closed, to avoid congesting the bandwidth. Ministry C has a network connection with a bandwidth of approximately *"120 kilobytes per second to 512 kilobytes".*

Nevertheless, the interviewee from Ministry C wishes for a connection between ministries and departments that use similar records. The interviewee stressed that *"there is a need to share resources and integrate because we want the same person at the police station"* who is recorded in their systems, instead of capturing all the data from the start.

2. Biometrics technologies in use

Biometrics technologies in use at Ministry C include fingerprints based systems. All nine (9) respondents who completed the questionnaire indicated that they use fingerprint based biometrics at Ministry C. However, a facial is also used manually as employees compare an individual's face in the ID against the ID holder. In addition, Ministry C intends to add iris biometrics technologies to the current fingerprint based system. The interviewee explained on the need for the iris: *"we are planning to implement the iris for the reason that if one is unable to use fingerprints, one has an option to use the iris."* The interviewee confirmed that they intend to use both the fingerprints and iris biometrics based system. The interviewee explained the use of multimodal biometrics by stating that: *"That's why we are not phasing out fingerprints. We will use the combination of both (fingerprints and iris)."* Biometrics at Ministry C are mostly used for CPA (confirmed by seven respondents), followed by API as confirmed by three respondents, then VoF as confirmed by three respondents and lastly APD as indicated by two respondents who completed the questionnaire.

3. *Biometrics challenges*

A number of biometrics challenges were noted from the data collected through the interviews and questionnaires. In particular to the interview, the interviewees indicated that they face challenges associated with the use of biometrics technologies, among them the costly bandwidth. Costs are seen as a challenge for both the use and implementation of biometrics. This is necessitated by the stakeholders who do not seem to really understand the importance of biometrics. The interviewee explained: *"when it comes to implementations, the main challenge is only finance of the budget. The budget is a constraint. The stakeholders seem to not really understand the biometrics importance."* In addition, the fact that biometrics technologies are not locally manufactured and sourced is seen as a challenge that contributes to the total cost and delays in the delivery of the equipment. The interviewee stated that: *"you find that hardware you have to procure from outside and they are very expensive and it also takes long to get delivered."*

It was also noted through the interviews and questionnaires that at times scanners fail to capture the fingerprints of individuals due to the fact that some people are disabled while others' hands have damaged fingerprints due to manual work. The interviewee explained the challenge: *"The challenges are that most of the Namibian citizens are doing hard labour so hands are damaged so to get a good quality image is a challenge or you get someone without a hand, therefore you can't take fingerprints".* This challenge was also confirmed by one of the respondents who completed the questionnaire. The interviewee also noted the challenge to find people with *"skills or expertise in the area"* of biometrics. Other challenges that were raised by data gathered through the questionnaire are as follows:

- Three respondents indicated that the fingerprint system often gets affected by power outages
- One respondent highlighted that some offices are not networked, meaning that individuals working at Ministry C require different access mechanisms to have physical access to those offices

4. ***Biometrics necessity***

In particular to the need for biometrics, the interviewee expressed their necessity within their Ministry. The interviewee for Ministry C highlighted that it would be good to engage the iris together with fingerprints. In relation to the iris, the interviewee found it very suitable to their ministry which involves the evaluation of vehicle drivers. The interviewee explained how the iris would suit their needs: *"Yes I feel they are necessary and we prefer the iris for we deem it to be more fit and practical for our business requirements, mainly the driver's licenses, so every driver needs to be able to see, so if they can see, you can identify them with the eye."*

5. ***Viable maintenance policy***

Data related to the presence of an IT maintenance policy and how often they do routine checks was also collected. Accordingly, the interviewee confirmed that they have an IT maintenance policy that is generic to IT equipment like scanners and PCs which are done on a monthly basis. The interviewee explained how the maintenance of IT equipment is done at Ministry C: *"Yes we have an IT maintenance policy and do routine checks in place. Like I said it's generic to IT equipment, printers and PCs. For when someone is doing a maintenance check, they check the scanner, dust it, clean and see if it's working. Our routine checks are normally monthly, like every month a person has to do preventive and maintenance on the hardware; for software we normally do whenever a batch comes up."*

4.3.2.2 Political and Government aspects:

Findings on the political and governance aspects which include policies and stakeholders are outlined below:

1. ***Policies***

Data was gathered to evaluate how Ministry C's IT polices and plans support the implementation of biometrics. Findings from Ministry C through the interview show that the ministry has a generic IT plan in which biometrics is seen as part of IT. The interviewee explained: *"our plan is mainly generic to IT, we regard biometrics as an IT, for example the finger print reader, we regard it as ICT hardware, therefore we only apply but we don't have a specific plan that is to biometrics."* Ministry C's IT plans ensure *"ICT system availability in terms of infrastructure, Network and*

Applications." As such, the IT plan supports biometrics systems by making sure that they are always available at all times to avoid interruptions to the business.

In addition, data was gathered to establish the steps followed by Ministry C in implementing their biometrics. It should be noted that Ministry C started implementing the biometrics around 2005 - the fingerprint system. At that time, Ministry C borrowed ideas from countries that had already implemented biometrics in order to plan on how to implement biometrics. The interviewee explained: *"The previous implementation* (referring to the time they implemented biometrics for the first time) *we did not have a model, we sort of benchmarked from neighboring countries that were using the same technology and we took it over."*

Nevertheless, Ministry C is adopting a different approach to the implementation of biometrics this time around. The Ministry hired an IT expert (IT researcher focusing in biometrics, who has a Doctorate) to assist in the implementation. The interviewee explained how the hired expert is assisting in coming up with the IT plan: *"at the moment we hired a biometric expert* (Namibian in the UK) *who did an analysis on our needs and came up with a clear implementation guideline which we will then intend to use for the implementation but the governance and the maintenance of it is still no clear guidance."*

2. Stakeholders

Data related to important stakeholders in the project of biometrics was collected. The interviewee identified the following stakeholders:

- The government
- The community, road users whose fingerprints are being scanned. The interviewee explained the role of individuals: *"Their role is that without them we can't really get their fingerprints. We have to take care of their interests because for example they risk things like identity theft."*
- The law enforcement - the interviewee explained that the law enforcement *"ensures that the people being issued with the driver's license are indeed the owners hence the need for biometrics verifications to identify the person."* The interviewee further indicated that the

law enforcements "*do finance us (Ministry C) for doing those functions*." While the ministry appreciates the financial support given, they however feel that *"the stakeholders seem to not really understand the biometrics importance"* hence the budgetary constraints they are facing in relation to biometrics acquisition and implementation.

4.3.3. Summary of Ministry C findings

Table 5: Summary of findings from Ministry C

Technology Aspect	**Biometric traits in use:**	− Fingerprints, − Facial
	Biometrics need	− Shown the need of biometrics
	Biometric challenges	*Technical challenges:* − Not applicable on handicapped. − Failure to capture fingerprints of manual laborers − Lack of skills and expertise − Not enough computer network coverage *Economic challenge* − Costs: bandwidth costs; biometrics initial, implementation and use costs *Other challenges:* − Long deliveries − Easily affected by power failures − Lack of adequate government support
	IT infrastructure	− Viable wide area computer network − Equipped with servers and storage devices

		− Use a Multiprotocol Label Switching (MPLS)
	Maintenance policy	− Use IT policy on biometrics
The political and governance aspect	**Policies**	− Use the IT policy on biometrics
	Stakeholders	− The government support − Community − Law enforcement

4.4 Conclusion

The chapter presented empirical evidence from data collection. Data was collected using interviews, questionnaires, observations and document analysis. Data for each ministry (case) was displayed separately indicating what was found at each case. The display of findings from each case included a brief overview of each ministry concerned in order to enhance the understanding of the case’s setting or context. Three ministries were considered for data collection. Data outlays within each ministry was analysed following the aspects of the ICT roadmap theoretical framework, namely the technological aspect and the political and government aspects.

These findings shall be analysed together in the next chapter.

CHAPTER 5: CROSS-CASE ANALYSIS AND IMPLICATIONS

The chapter undertakes a cross-case analysis, thereby collectively reporting findings from all cases or ministries considered. Findings from data analysis are compared with findings in the current literature to identify similarities and differences.

5.0 Introduction

The previous chapter did a within-case data analysis and presented the findings from each ministry separately. This chapter proceeds with data analysis by conducting a cross-case data analysis of data collected using the methodology of chapter three. The chapter combines findings from all ministries that were considered during data collection. The aim is to identify constructs from all ministries considered and design a framework of biometrics implementation in the Namibian ministries. In addition, data collected through Likert based questions is used to support findings from interviews. Cross-case analysis is done within the aspects of the ICT roadmap theoretical framework, namely the technology, political and governance, economic and social aspects as proposed by Jere et al. (2012). It should be noted that the ICT roadmap theoretical framework was used as a guideline during the development of the data collection instrument. The focus in this research was mainly on the technological aspects of the multimodal framework. The chapter provides an analysis of the findings and relates the findings to current literature.

5.1 Cross-case analysis

The aim of the cross-case analysis is to consolidate findings from all ministries considered. The cross-case analysis is conducted by analyzing similarities and different findings from all ministries considered. Data collected using Likert based questions is used to support findings from the interviews. The aim is to put together views of senior management that were engaged through interviews and junior staff members whose views were gathered through the use of a questionnaire. Junior staff members' views are considered since they are the ones who are involved in the day to day use of biometrics. Cross-case analysis is done within the aspects in the ICT roadmap theoretical framework.

5.2 The technology aspects

This section presents findings that relate to the technology aspects of the ICT roadmap methodological framework. It looks at biometric factors of adoption and use that aligns to the technology aspect.

5.2.1 Biometric use

All ministries engaged indicated that they are using biometrics within their organisations. However, some ministries have started with unimodal biometrics based systems and now moving towards multimodal biometrics. The fingerprint is the common biometrics trait used across all ministries considered. Nearly all ministries engaged implemented the fingerprint system through AFIS. However, besides using fingerprint based biometrics, ministries have different alternative biometrics traits which they use, while others are currently in the process of moving from unimodal to multimodal biometrics. Common traits for biometrics securities within the surveyed ministries include fingerprints, face, iris, voice, hand geometry and signature. In addition, the majority of participants prefer the use of fingerprints, face and iris as biometrics traits for multimodal biometrics systems within their organizations as shown in Figure 7.

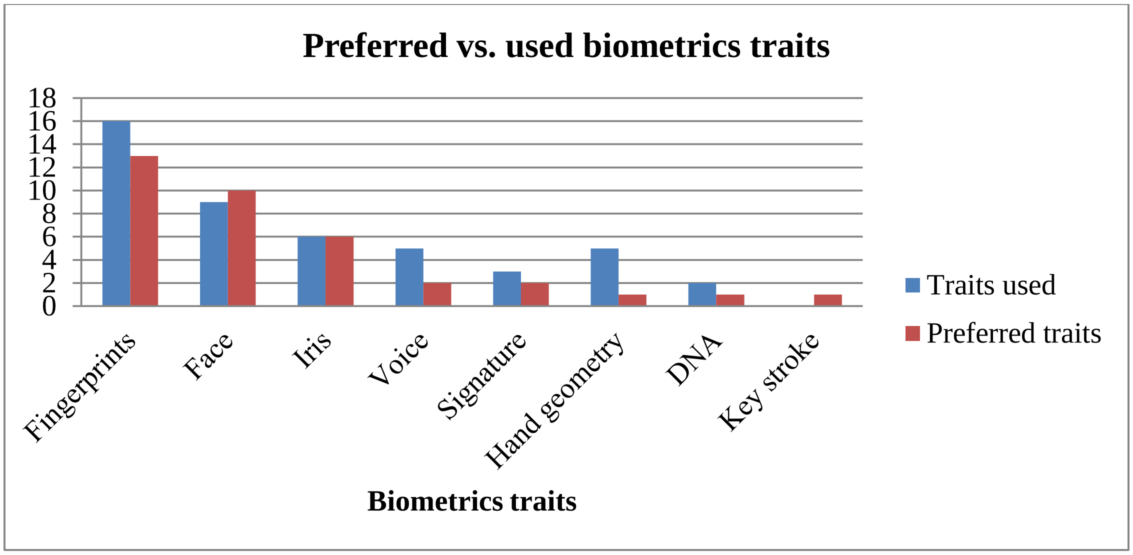


Figure 7: Preferred vs. used biometrics traits.

For instance, one of Ministry A's departments has multimodal biometrics systems that are based on fingerprints, iris and voice. The interviewee explained the reasons behind engaging multimodal biometrics: "*…you don't want to touch equipment while you are in analysis with your fingerprint and you can't because you are normally gloved up and you can't activate such a reader with that (fingerprint) so we resort to iris technology and in certain instances we resort to voice so we use them all as we go along.*"

On the other hand, Ministry B is currently using fingerprint based biometrics. However, plans are underway of engaging biometrics technologies that use face recognition. In addition, Ministry C is also using fingerprints based biometrics systems and they also have plans to engage iris based biometrics. The aim is to use both fingerprints and iris. The use of multimodal biometrics could be motivated by the challenges faced by Ministry C, among them being when the fingerprint based system fails to capture fingerprints of manual labourers as explained under biometrics challenges. Common uses for biometrics across all ministries include CPA (14), VoF (9), API (5) and APD (5). These findings on uses and users of biometric systems conform to propositions by the National Science and Technology Council (2011), that as in 2006, the primary users of biometrics technology are large government identification systems used by law enforcement, national security, military and border control (immigration management).

5.2.2 Biometrics challenges

The gathered data across ministries show a number of challenges faced during the implementation of multimodal biometrics. When compared to multimodal biometrics, participants feel there is not much difference in terms of the magnitude of challenges associated with unimodal biometrics. 35% (6 respondents out of 14) have a neutral perspective on the fact that unimodal biometrics face more challenges than multimodal. 24% (4 participants) and 12% (2 participants) strongly agree and agree respectively that unimodal biometrics face more challenges than multimodal. This could be attributed to the fact that the majority of ministries implemented unimodal biometrics first and they are now gradually engaging multimodal biometrics. These challenges include costs, interoperability, failure to capture prints, false rejection, lack of biometrics skills and knowledge, acceptance and use of biometrics, infrastructural challenges and other challenges. These challenges are discussed below:

Costs - all ministries engaged showed that the costs of biometrics technology are a hindering challenge. These costs include costs of buying the equipment for the first time, doing maintenance and replacing equipment that would have over lived their life-span. This is further exacerbated by the fact that stakeholders who finance the biometrics *"seem not to really understand the biometrics importance"*, hence it is often allocated an insufficient budget. Another factor contributing to the overall cost of biometrics technology is the fact that the equipment is not locally manufactured here in Namibia. Instead, it has to be imported from other countries. These findings are supported by data gathered using the questionnaire as 35% agree, with another 35% of the participants strongly agreeing that biometrics technologies are expensive. 24% have a neutral view, while 6% strongly disagree that biometrics technologies are expensive. In addition, 41% strongly agree, with another 41% agreeing that biometrics deployment requires a good budget. In addition, findings from other research on biometrics confirm that biometric costs as a challenge. For instance, Jain and Kumar (2010) noted that deploying biometrics is associated with direct and indirect costs. Direct costs include the cost of hardware components (sensors, processor, and memory) and software modules (Graphical User Interface and matcher). Indirect costs include system installation, training/maintenance requirements and user acceptance.

Interoperability - one concern that was raised is the issue of compatibility among the biometrics equipment from different suppliers or manufacturers. One interviewee from Ministry A explained:

"You are often faced with the end of life product cycles, where you have to replace products. Once you do that you are immediately informed that the new camera that has now been replaced was for the previous system that has now become redundant. One can imagine if your interface connectivity, that mechanism architecture changes you will have to effect those changes at a greater cost so I think cost is a big issue." Jain and Kumar (2010) noted that a biometrics system can no longer operate under the assumption that the same sensor, same algorithms, or same operating conditions will always be available during its lifetime. As such it would be good if biometrics systems are highly interoperable to authenticate individuals using sensors from different vendors and on varying hardware/software platforms (Jain & Kumar, 2010). Accordingly, standards have matured significantly and have contributed to improved system and biometrics device interoperability (Science and Technology Council, 2011).

Failure to capture fingerprints - all ministries engaged mentioned that some biometrics technologies are difficult to implement as they are not applicable in certain situations. All ministries highlighted that fingerprint based biometrics are difficult to use when dealing with handicapped people and manual labourers. This is a big concern given that one of the main uses of biometrics by all the ministries considered is for the identification of individuals or verification of one's identity. These findings agree with studies already conducted in the field of biometrics. For instance, a study on biometrics use in India by Mukhopadhyay, Muralidharan, Niehaus and Sukhtankar (2013) show that the first few months of user enrolment is usually associated with software glitches, errors and malfunctioning fingerprint readers. In addition, Unar, Seng and Abbasi (2014) also noted that imaging sensors are often unable to acquire the valid biometric sample. Very often, such errors prevail amongst the systems requiring impression based imaging of the modalities automatically (Unar et al., 2014). However, in the USA, the US government has supported technology testing and standards development, creating frameworks and a strong stimulus for continued technological improvement through coordinated and focused research and product development (Science and Technology Council, 2011). As already noted, the post office's service provider involved in a biometric payment system in India replaced their fingerprint readers with a more sensitive version of the device in order to minimize technical problems with fingerprint reading, something that suggests the availability of good sensors or cameras (Mukhopadhyay et al., 2013). On the other hand, challenges like these have forced ministries into engaging multimodal biometrics, whereby if one biometric trait is not viable, they would use another trait or use both traits, for example using fingerprints and iris. In some instances, manual operations override the technical system where possible.

False rejection - two ministries (Ministry A and B) indicated that users are often subjected to false rejections as the fingerprint based system rejects users that already exist in the system. Users are often forced to do multiple tries till their prints are recognised. A false rejection compromises one of the biometric systems' recommended characteristics or attributes that contribute to its overall performance (Jain et el., 1998 as cited in Bours, 2012). Accordingly, Mukhopadhyay et al. (2013) noted that agents often override the use of biometric based Point of Sale readers due to the system's failure to recognize fingerprints of older beneficiaries or manual labourers (in both cases, fingerprints may be significantly worn down). Normally, these errors occur due to dirty surfaces of the imaging sensors (Unar et al., 2014).

Lack of biometrics skills and knowledge - All ministries highlighted the lack of people with biometrics skills. For instance, one participant from Ministry B indicated that the biometrics systems often malfunction due to user miss-use, something that could result from the lack of knowledge on how to properly handle the equipment. In addition, the lack of biometrics skills and knowledge might have motivated Ministry C into hiring a biometrics research expert based in the United Kingdom to assist them in evaluating their needs for biometrics and how to implement it. The lack of people with biometrics skills is also common in the literature. Agents in the province of Andhra Pradesh complained about the lack of available technical support when malfunctions do occur, an issue which must be addressed by the responsible service providers (Mukhopadhyay et al., 2013). On the other hand, participants from Ministry A noted that quite often their departments focus on the biometric equipment or systems with little attention paid to the training of employees on how to operate these biometrics systems. To a certain extent, such issues negatively affect the acceptance of biometrics within the department as explained in the next section. The need for biometrics skills and knowledge was also confirmed in the questionnaire as 24% strongly agreed and 24% agreed that biometrics deployment requires training and regular refresh courses. 12% had a neutral view while 18% disagreed on the fact that biometrics deployment requires training and regular refresher courses.

However, data collected through the questionnaire suggests that all users do not need technical skills on biometrics technologies. 47% disagreed while 29% of the participants strongly disagreed on the need for biometrics technical skills to all users. Only 12% strongly agreed that it is important for all users to have biometrics technical skills. This could imply that users may require training on the basic uses of biometrics, not a deep technical part of it. Rather, technical training on biometrics can be limited to technical people or staff in the IT department. The Andhra Pradesh government of India adopted a similar approach of training identified agents who facilitated the implementation of a biometric payment system (Mukhopadhyay et al., 2013). The training lasted for two to seven days, focusing on equipping the agents with knowledge on how to operate Smartcard readers, downloading and updating data and maintaining records. Jain and Kumar (2010) also noted that new user enrolments in a large-scale biometric system will typically require periodic re-training or updating of the matcher.

Acceptance and use of biometrics - only Ministry A expressed concern over the acceptance and use of biometrics. The interviewee from Ministry A indicated that employees of this ministry do not see the need for biometrics; they feel its *"too much extra trouble".* As a result quite often they deactivate the biometric systems and use manual systems, especially on fingerprint based doors. In addition, Ministry A faces the challenge of inter-ministerial acceptance of biometrics. Thus, biometrics are found in other ministries while other ministries are still lagging behind, making its universal acceptance across Namibian ministries a challenge. This is a big concern for Ministry A, considering the fact that its mandated tasks involve working with other ministries, in particular the Ministry of Justice. One of the interviewees from Ministry A explained the challenge as follows: *"The constraints in all of these are not the technology. It's not the rules governing this. Rather it is the legal system and we find that increasingly so when we go to courts of law. They lag behind tremendously, and courts tend to be very pedantic and they often argue about the validity of these* (referring to the use of biometrics traits like facial, hand and ear geometric to identify someone). *So that will be the big challenge in the future to see how we can sensitize the courts, how we can sensitise judges and presiding officers even if they don't understand technology to accept it".*

Considering that, only Ministry A indicated problems with user acceptance, this could be attributed to the fact that biometrics are still new to the staff of Ministry A. It should be noted that Ministry A is currently rolling out its biometrics and as such the levels of acceptance are still low with staff yet to get used to the new change. This could explain why there are mixed views on the levels of user acceptance for using biometrics in Namibia. 12% and 12% strongly agree and disagree respectively on the subject that the user acceptance of biometrics in Namibia is very low. In addition, 29% and 29% agree and disagree on the fact that the user acceptance of using biometrics in Namibia is very low, while 18% have a neutral view on the subject. Nevertheless, biometrics acceptance has always been a cause for concern in countries that have implemented the technology. In India, staff members involved in the project of biometrics conducted multiple workshops with district and other local authorities, in order to educate them about the Smartcard project and their role in the implementation chain (Mukhopadhyay et al., 2013).

Lack of infrastructure - Ministry A and C expressed infrastructural related challenges. These include the lack of a wide area network covering all centres and electricity problems. For instance, Ministry A mentioned that it is a challenge to implement biometric systems when the network is decentralized with centres not networked together. Similarly, Ministry C also indicated that some offices are not networked, making it impossible to use biometric systems. Lastly, only Ministry C indicated that their biometric systems often get affected by power outages.

Other challenges - other challenges that were noted by individual ministries are as follows:

- Ministry A agreed that biometrics technologies involve different technologies with different product life cycles that bring in compatibility challenges.

- Ministry B highlighted that there are challenges with regular maintenance as the system malfunctions due to user miss-use

5.2.3 IT Infrastructures

All ministries confirmed the need for a viable IT infrastructure for the implementation of biometrics. Commonly used infrastructures include computer network, servers, scanners, cameras and software with a reliable and redundant database as one of the elements. These biometrics and IT infrastructures identified through data collection concur to those identified in the literature. As Unar et al. (2014) have highlighted, that every biometrics system comprises of an image acquisition module: this acquires the image of a biometrics trait and submits it to the system for further processing; feature extraction module: processes the acquired image thereby extracting the salient or discriminatory features; matcher module: matches the extracted features of the probed image with those of a gallery image to obtain a match score whereas; an embedded decision making module verifies or rejects the claimed identity based on the match score and a database module: contains the digital representation of previously acquired samples, very often termed as templates.

However, in terms of infrastructure, another important element is the speed at which the information is to be extracted, processed and results delivered.

In this regard, 18% strongly agree and agree, while 24% have a neutral view on the fact that multimodal biometrics can improve the speed and accuracy of biometrics. In addition, one interviewee from Ministry A highlighted that even though they have face and ear geometry biometrics system, they *"do not use it often because it takes a lot of time"*. In support of these findings, Jain and Kumar (2010) stressed that UIDAI's project of creating India's billion plus population biometrics database will require highly efficient indexing techniques for the system to be efficient. These views arguably go hand in hand with respondents' views who acknowledge that biometrics implementation requires a large database space as 24% strongly agree and agree to that.

In addition, all ministries make use of AFIS for the identification of individuals among other things. This is commensurate with the literature as Jain and Kumar (2010) acknowledge that "Now, virtually all law enforcement agencies worldwide use Automatic Fingerprint Identification Systems (AFIS)". AFIS was initiated in the 1960s by the FBI in the United States, the Home Office in the United Kingdom, Paris Police in France, and the Japanese National Police with the aims of developing an automated fingerprint identification system that could classify, search, and match ten print cards used for personal identification (Moses, 2011).

Even though all ministries appear to be using and requiring the same infrastructure, the collected data suggests that there is limited or no network connectivity among ministries. One interviewee indicated that "*there is a need to share resources and integrate them because we want the same person at the police station.*"

5.2.4 Biometrics necessity

All ministries engaged see the need for multimodal biometrics as it assists them in the conduct of their mandate. Biometrics are considered useful in identifying individuals, controlling access and even curbing forgery among other things. Data collected through the questionnaire shows that 78% of participants strongly agree that multimodal biometrics can improve security and identification. A committee on biometrics standards during the UIDAI project of developing the unique identification number for every Indian considered that face, all ten fingerprints and both iris scans are useful biometrics traits for unique identification (UIDAI, 2010).

In support of the multimodal biometrics, 22% strongly agreed and 17% agreed that combining finger prints and facial images can improve the security of biometrics. These beliefs on the effectiveness of biometrics somewhat explain why 41% of the participants disagree that some users lack trust in using biometrics technologies, with 35% having a neutral view on trust. All these findings suggest the importance and need for multimodal biometrics.

When participants were asked to compare unimodal against multimodal in terms of reliability; 22% strongly agreed that the unimodal systems are less reliable, 17% agreed that unimodal systems are less reliable, with 28% participants' view being neutral. This finding further affirms the need for multimodal biometrics because of their reliability in terms of efficiency. Accordingly, Unar et al. (2014) acknowledge that multimodality based systems offer better accuracy as compared to unimodal systems. Similarly, Jain and Kumar (2010) state that multimodal biometrics systems offer higher accuracy and can also address the problem of non-universality. Careful selection is the key point to success since selecting the modalities belonging to one region may not be a good choice because an accidental loss of that organ will result in the user's inability to submit the required signature (Unar et al., 2014).

In addition, when asked to evaluate the need for biometrics in the public sector, 11% strongly agreed that multimodal biometrics are needed in the public sector, 33% agreed on the need of multimodal biometrics while 11% were neutral, with 28% not agreeing on the need for biometrics in the public sector. This could be attributed to the less penetration and use of biometrics in Namibia. Nevertheless, studies across the globe affirm the need for biometrics systems in the public sector. For instance the US's National Science and Technology Council (2011) states that as in 2006, the primary users of biometrics technology are large government identification systems used by law enforcement, national security, military and border control (immigration management). Similarly, Unar et al. (2014) recently noted the use of biometrics by most governments in the Asian Pacific region, for example the issuance of a multi-biometric National Identity Card and Passport scheme in Pakistan, Bangladesh government's high security driving license scheme, and the Indian government's Aadhaar/Unique ID project which has been ranked as world's largest biometric project.

5.2.5 Viable maintenance policy

In all ministries engaged, there is no specific maintenance policy for biometrics. Biometrics is seen as an IT component hence it is covered by the IT maintenance policy. For instance, Ministry B has a maintenance policy for individual hardware and software. The policy also extends to biometrics which is seen as a part of IT. However, both departments under Ministry A indicated the importance of having a biometric maintenance policy in order to have a smooth maintenance procedure. As such, the heads of IT in departments under Ministry A are currently working on crafting the maintenance policy for biometrics.

In addition, all ministries indicated that multimodal biometrics require regular maintenance. However, not all ministries indicated how often they do their regular maintenance on multimodal biometrics. For instance, Ministry A just indicated that it has to be *"more frequent."* Ministry B pointed out that their maintenance plan, which involves routine checks and troubleshooting are done depending on the system performance. These findings suggest that while a maintenance policy might be in existence for Ministry A and B, they have no specific dates or times they do their maintenance, something that calls for a specific maintenance policy that is clear to ensure responsibility and accountability. Nevertheless, only Ministry C indicated that they do a monthly maintenance of their IT equipment including biometrics. The interviewee explained that: "*our routine checks are more normally monthly, like every month a person has to do preventive and maintenance on the hardware*". In addition, participants were asked for their views on multimodal biometrics' need for regular updates. About 28% strongly agreed that multimodal systems require regular updates, 28% agreed that multimodal systems require regular updates, with only 22% having a neutral perspective.

5.3 Political and governance aspects:

5.3.1 Stakeholders

Ministries identified similar and different stakeholders of their multimodal biometrics. All ministries identified the government as a stakeholder. When it comes to government support as a stakeholder, Ministry B feels they do not get any advice on how to implement biometrics, while Ministry C feels that the government does not really understand the importance of biometrics, hence they often get limited financial support towards biometrics. Literature on biometrics implementation shows that the government's support is very crucial for its success. For instance, the USA and Indian governments are actively involved in their biometrics projects, giving financial support, research institutions, drafting polices on standards and what biometrics to use, coming up with implementation monitoring teams, coming up with committees for biometrics standards and engaging biometrics experts (Mukhopadhyay et al., 2013; National Science and Technology Council, 2011; Unique Identification Authority of India, 2010).

Ministry A identified their IT Department as a stakeholder. On the other hand Ministry B identified a department in Ministry A as a stakeholder and indicated that they work together as they are somewhat *"connected"* together via a network that they share.. Ministry B went on to highlight the role of commercial businesses as they have an influence on what biometrics Ministry B should adopt and use. Lastly, Ministry C identified the community and law enforcement entities as stakeholders in addition to the government itself as a stakeholder. These findings agree with the literature as in most instances, biometrics implementation and use involves the community, banks, the government (Mukhopadhyay et al., 2013) and different government departments interrelating with each other as they will be using the same biometrics data base (National Science and Technology Council, 2011; Unique Identification Authority of India, 2010).

In addition, participants were asked if they feel that stakeholders in Namibia are promoting biometrics deployments and working together. The majority (47%) of participants had a neutral perception, while 24% did not agree that stakeholders are promoting biometric deployment. In addition, 35% disagreed that stakeholders are working together, while 35% had a neutral perspective. Only 12% agreed and strongly agreed that stakeholders are working together in relation to biometrics implementation. This could be explained by the limited finance and advice from the government as highlighted above. In addition, one of Ministry A's departments indicated that other departments for example in the *"courts"* and *"judges"* are yet to buy into the biometrics adoption and use in Namibia. Consequently, 41% of participants strongly agreed and agreed that stakeholders should engage each other during biometrics implementations.

5.3.2 Policies

Nearly all ministries (except one department under Ministry A) have no policies or plans specific to multimodal biometrics implementation and use. Biometrics are seen as a part of IT and as such, plans and polices supporting biometrics are found within the IT plans and strategic plans that are in existence. Only one department under Ministry A has a biometric implementation policy. In terms of polices, literature shows that plans and polices need to be drawn in advance for the successful implementation and use of biometrics. For instance the Indian government developed a statutory body - the UIDAI that is responsible for creating, administering and enforcing policy, prescribe guidelines on the biometric technology, the various processes around enrolment, and verification procedures to be followed for its unique identification project for Indian residents (UIDAI, 2010). Among other polices or plans that were put in place included the identification and standardization of biometrics traits to be used, setting standards on demographic data to be collected and proposing the legal framework and addressing ethical issues. On the other hand, the government of Andhra Pradesh drafted a formal Memorandum of Understanding between stakeholders that included banks, the Department of Rural Development, and the Institute for Development and Research in Banking Technology (IDRBT) on how they would interrelate in the biometrics payment system (Mukhopadhyay et al., 2010).

Furthermore, all ministries demonstrated different biometrics implementation approaches. For instance, one department under Ministry A started the deployment of biometrics at the head office and moved on to other branches. Similarly, the government of Andhra Pradesh started the implementation of its biometrics payment system with a pilot survey that included all stakeholders (Mukhopadhyay et al., 2010). Nevertheless, when it comes to the planning on buying biometrics equipment, the department's approach is to make requests for the funds at the same time as the

Medium Term Economic Framework cycles, and the budgetary cycles in order to be assured of the availability of funds. Ministry B’s choices of what biometrics to implement and when is influenced by demands from other institutions such as banks and insurance companies. Once in place, the biometrics will be treated using the IT policy that is in place. Lastly, Ministry C borrowed the biometrics implementation approaches from reference cases of other countries that were using multimodal biometrics when they first implemented their biometrics around 2005. Ministry C mentioned that they have recently hired an IT research expert specialising in biometrics to advise them on how to deploy and use biometrics. This partly conforms to the international standards. For instance the US and India normally come up with committees and teams made up of experts in the relevant fields who are given the task of identifying the biometrics to use and all other concerns including legal and ethical issues.

All these findings suggest the importance of a biometrics policy, be it within the IT plan or as a standalone policy. However, participants through the questionnaire expressed mixed views when asked on the need for proper national policies for biometrics. About 24% strongly agreed, 24% agreed, 41% had a neutral view, while 11% disagreed on the need for national polices relating to biometrics implementation. Given that the majority agreed to the need for national polices, it is therefore concluded that national polices are necessary for the implementation of multimodal biometrics.

5.4 Conclusion

This chapter conducted a cross-case data analysis, thereby combining and presenting together findings from each ministry considered. Findings from data collection were compared with the current literature on biometrics to identify similarities and differences. The conduct of cross-case data analysis was done within the aspects of the ICT roadmap theoretical framework, namely the technology, political and governance, economic and social aspect. The technological aspect had major attributes as identified from data collection, namely biometrics in use, biometrics challenges, IT infrastructure, and viable maintenance policy. Attributes that were found through data analysis within the government and political aspect include stakeholders and policies.

Based on these findings, major components of the framework of multimodal biometrics implementations shall be identified in the next chapter, leading to the proposal of the framework.

CHAPTER 6: FRAMEWORK FOR MULTIMODAL BIOMETRICS

The chapter designs and proposes a framework of multimodal biometrics implementation in the Namibian government. The chapter identifies components of the framework based on findings of chapter 5 and goes on to propose a framework for multimodal biometrics implementations.

6.0 Introduction

This chapter focuses on explaining the components and the process followed in designing multimodal biometrics frameworks for the Namibian government. The chapter explains the rationale behind designing the framework for multimodal biometrics and discusses the main components that are the building blocks to the multimodal biometrics framework. The chapter goes on to outline the framework, indicating how the identified components interrelate. An overview of the proposed framework for multimodal biometrics implementation concludes the chapter.

6.1 The framework's rationale

Research on biometrics has been focusing on improving the performance of biometrics, coming up with new traits, applying biometrics in different environments and establishing challenges associated with biometrics implementation and use (AADHAAR, 2010; Jain & Kumar, 2010; Mukhopadhyay et al., 2013; National Science and Technology Council, 2011; UIDAI, 2010; Unar et al., 2014). However, little attention has been paid on designing technical frameworks that can be used as a source of guide by governments on how to implement multimodal biometrics within their different ministries and departments. This is critical to governments in developing countries where technology is yet to be totally understood and accepted. For instance, Ngcingwana (2008) mentioned that the value of ICT as a strategic enabler of provincial activities is not well articulated and is yet to be well understood, so as a result quite often the governments allocate insufficient budget towards ICT development. In this research the technical multimodal biometrics framework is proposed and this is from an academic point of view.

6.2 Multimodal biometrics framework designing process

The designing process of the framework for multimodal biometric implementation is guided by the secondary data of the literature review and the primary data that was collected through interviews and questionnaires from the selected ministries. Figure 8 shows the steps that were followed in designing the framework for multimodal biometrics for the Namibian government.

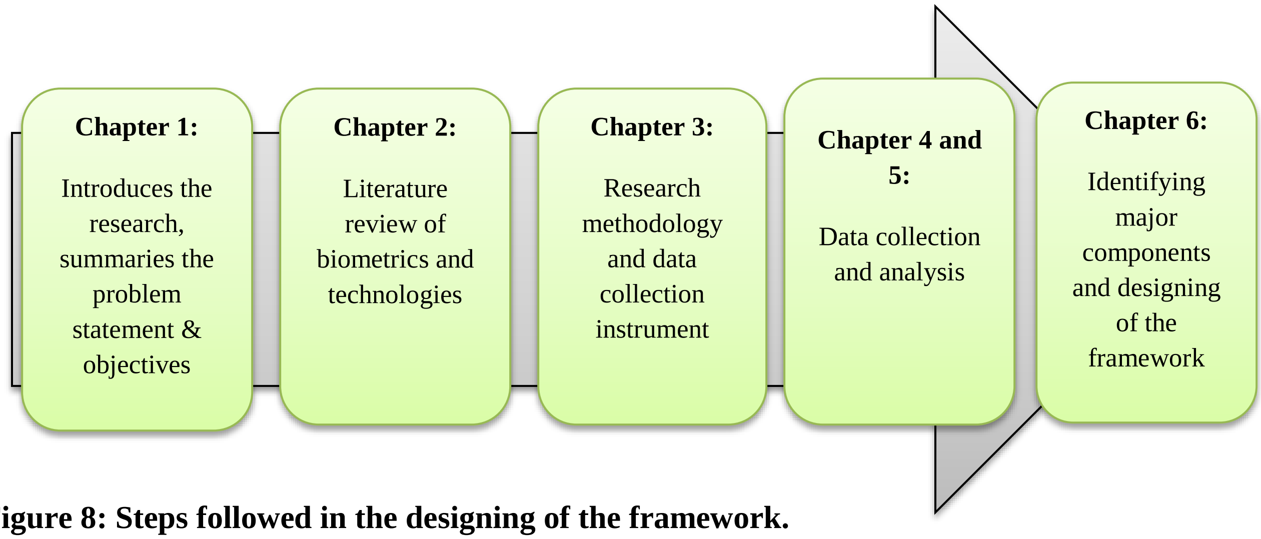

Chapter 1:
Introduces the research, summaries the problem statement & objectives
Chapter 2:
Literature review of biometrics and technologies
Chapter 3:
Research methodology and data collection instrument
Chapter 4 and 5:
Data collection and analysis
Chapter 6:
Identifying major components and designing of the framework

Figure 8: Steps followed in the designing of the framework.

6.3 Components of the multimodal biometrics framework

The components of the multimodal biometrics framework were derived from the data gathered using the research methodology of Chapter 3. The questionnaire and interview questions in the data collection instrument of Chapter 3's research method were guided by the technology roadmap theoretical framework extracted from Jere et al. (2012). The technology roadmap theoretical framework outlines local and global aspects that are to be considered when implementing technologies. As such, components of the multimodal biometrics framework were derived from attributes of the economic aspect, political and governance aspect, social aspect and the technology aspect that makes up the technology roadmap theoretical framework. The components were identified based on the assessment of the existing challenges and lessons that could be learnt from current biometrics implementations.

It should be noted that the main focus of this framework is on technological issues associated with biometrics implementation. This is critical to the certification of the intended qualification. As such, little attention is paid on other aspects like the social aspect and economic aspect with respect to the number of questions that were designed to evaluate these aspects in the data collection instrument. However, even if these aspects were not given much attention, it is true that they are very important in coming up with a sustainable multimodal framework and these were set aside as areas for future research. Based on the data analysis of Chapter 5, the identified components for the multimodal biometric framework include: the ICT infrastructure; biometrics architecture and technologies; multimodal biometrics technical skills; social acceptance; biometrics stakeholders; biometrics budget; monitoring, evaluation and updating; biometrics trends and emerging technologies; biometrics policies, implementation standards and plans. These components were identified in part to address issues raised through data collection and analysis in the previous chapters. These components are discussed in this chapter, outlining how they were arrived at and their role within the spectrum of multimodal biometrics implementation. These components are considered as the success factors to the implementation of multimodal biometrics in the Namibian government.

6.3.1 Multimodal ICT infrastructure

Data analysis and the reviewed literature show that a successful multimodal biometrics implementation requires a good ICT infrastructure in place, with the necessary hardware and software. This component was derived from the attributes of the technical aspects that were raised from data collection and analysis. These attributes include biometrics challenges (*lack of IT infrastructure, failure to capture fingerprints and false rejection*) that were identified and common *IT infrastructure* needed for biometrics, an attribute that was also identified through data collection and analysis as shown in Figure 9.

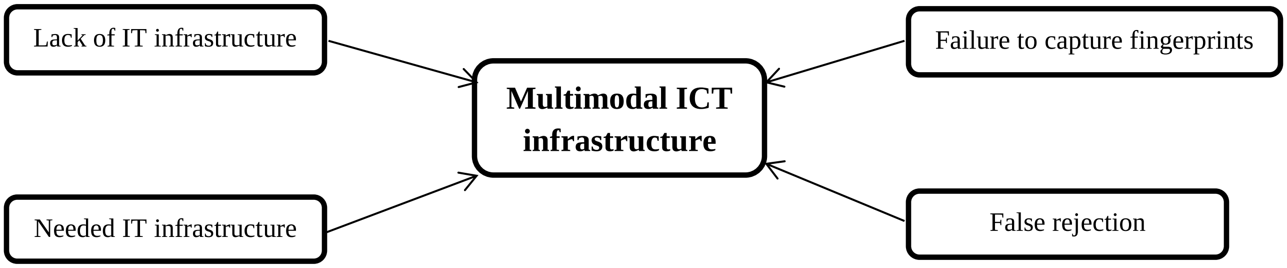
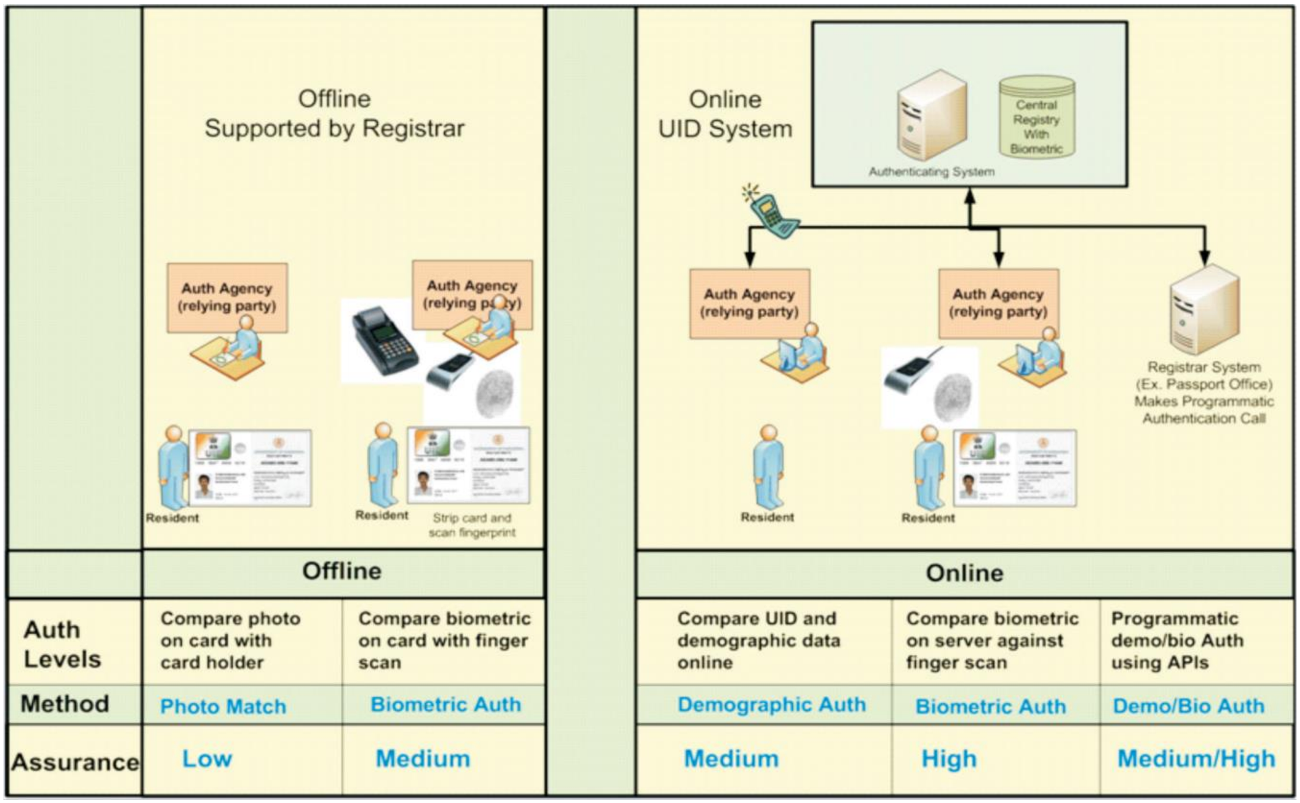

Lack of IT infrastructure
Failure to capture fingerprints
Multimodal ICT infrastructure
Needed IT infrastructure
False rejection

Figure 9: Attributes contributing to identification of the Multimodal ICT infrastructure

Multimodal biometrics infrastructure can include a reliable wide area computer network connecting all the departments and divisions involved, computer servers with database for storing templates, biometrics devices such as scanners and cameras, respective software that processes biometrics traits and electricity to power the infrastructure (Mukhopadhyay et al., 2013; National Science and Technology Council, 2011; UIDAI, 2010; Unar et al., 2014). In particular to biometric software, these can include the software that acquires the image of a biometric trait and submits it to the system for the extraction of salient or discriminatory features that would be used to match the extracted features of the probed image with those of the gallery image to obtain a match score. Examples include the AFIS that is fingerprint based and the Automated Biometric Identification System that maintains fingerprints, photographs and biographic information (National Science and Technology Council, 2011). Figure 10 shows an outlay of a biometrics system indicating how the ICT infrastructure can interrelate.


Offline
Supported by Registrar
Auth Agency (relying party)
Auth Agency (relying party)
Resident
Resident
Strip card and scan fingerprint
Online
UID System
Central Registry With Biometric
Authenticating System
Auth Agency (relying party)
Auth Agency (relying party)
Registrar System (Ex. Passport Office) Makes Programmatic Authentication Call
Resident
Resident

	Offline		Online		
Auth Levels	Compare photo on card with card holder	Compare biometric on card with finger scan	Compare UID and demographic data online	Compare biometric on server against finger scan	Programmatic demo/bio Auth using APIs
Method	Photo Match	Biometric Auth	Demographic Auth	Biometric Auth	Demo/Bio Auth
Assurance	Low	Medium	Medium	High	Medium/High

Figure 10: Multimodal ICT infrastructure outlay (source: UIDAI, 2010, p. 27).

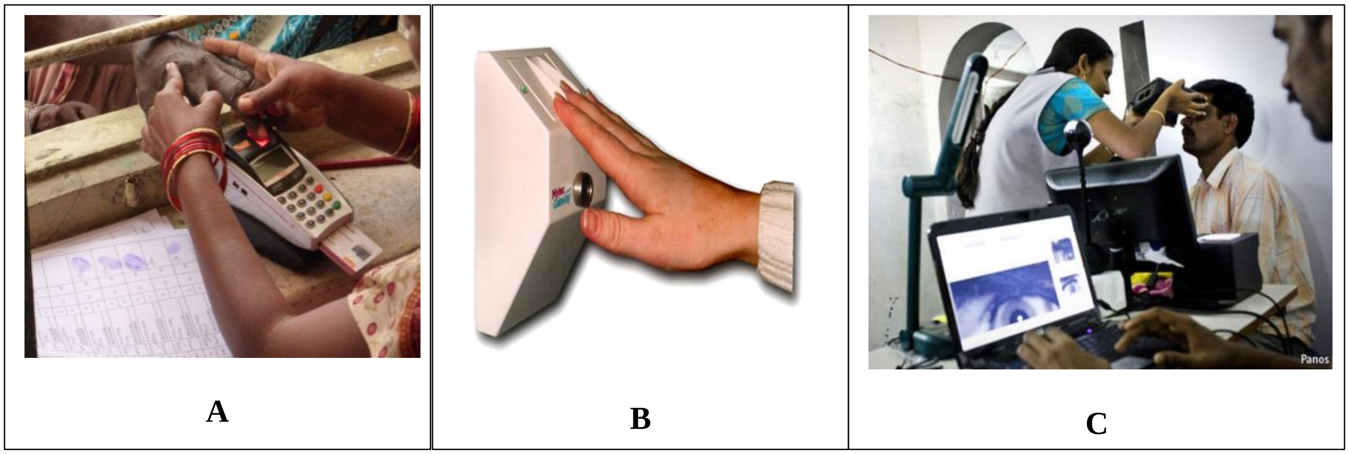


Figure 11: Multimodal biometrics equipment onsite (Mukhopadhyay et al., 2013; Yadav, 2013).

Figure 11 shows some of the biometrics equipment onsite that can be used in an online or offline setup. Picture A shows a fingerprint based biometrics system that works together with a smartcard in an offline setup. Picture B shows another fingerprint system that uses four fingers while picture C shows equipment for the iris based biometrics system.

6.3.2 Biometrics architecture and technologies

The biometrics architecture and technologies component was derived from the attributes of the technology aspects that were discussed in the previous chapter. These attributes include *biometric use*, *interoperability* and some elements from the biometric *IT infrastructure*. The biometrics system architecture can adopt centralized and decentralized network architecture depending on the uses of biometrics with different combination biometrics traits in use. The collected data shows that the Namibian ministries use biometrics for controlling the physical access to its premises, accessing personal devices, accessing personal information and the verification of information or identity. As such, biometrics systems for national purposes like the verification of residents' identity could be centralized at Ministry B. For instance, India's UIDAI through the Central Identities Data Repository (CIDR) manages the issuing of unique identity number based on multimodal biometric traits. All other organizations connect to the CIDR for identity verification purposes where necessary. Accordingly, all other institutions like banks and other government departments with biometrics systems can be connected to Ministry B and get online identification of residents as shown in Figure 12. However, the system can also be deployed in an offline environment whereby biometrics devices in use have several key features such as a slot for swiping a smart identification card, a fingerprint reader, and a display screen, something that would allow the comparison of scanned fingerprints of the cardholder to the biometrics stored on the identification card issued by Ministry B.

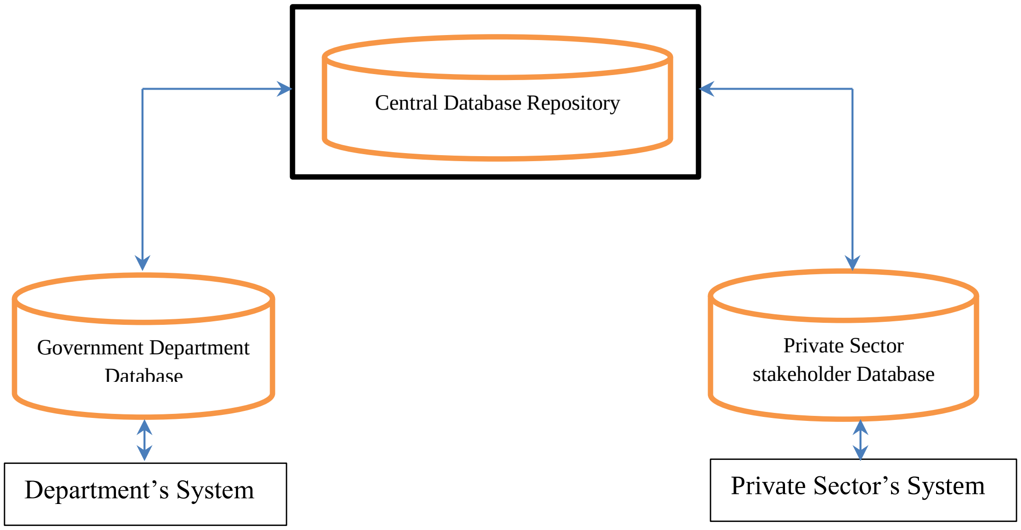

Central Database Repository
Government Department Database
Private Sector stakeholder Database
Department's System
Private Sector's System

Figure 12: Biometrics architecture for resident identification

On the other hand, localized operations like controlling physical access to premises, accessing personal devices and personal information using biometrics systems can have its repositories decentralized according to ministries or government departments. This is so because different ministries and government departments may require different biometrics traits for their systems. Besides, these ministries are allocated different budgets; hence they will not be able to afford the same equipment. Similarly, the US government and its departments have different decentralized multimodal biometrics systems, even though their systems are interlinked with prescribed privileges on what to access and edit.

However, with respect to the biometrics combinations of biometrics traits to use for multimodal biometrics, the majority of participants suggest the use of fingerprints, face and iris. Based on the collected data, biometrics traits that can be used for multimodal securities could include fingerprints, face, iris, signature, hand geometry and DNA. The choices and combinations of biometrics traits for multimodal biometrics depend on the needs of the organisation and the extent of risk. For instance, where the level of risk is too high, it is important to engage a combination of biometrics traits with greater universality and uniqueness such as fingerprints, iris and face. However, where there is limited risk, selected universal and unique biometrics traits could be used whereby one biometrics trait would be used under circumstances where alternative biometrics traits can't be used. For instance, Ministry C can use both iris and fingerprints but only use the iris if an individual does not have fingerprints. The policies section below explains further on precautions that need to be observed when implementing multimodal biometrics.

6.3.3 Multimodal biometrics technical skills

The implementation of multimodal biometrics requires that the affected people be given the necessary technical skills. Attributes contributing to this component include biometrics challenges (focusing on *lack of biometrics skills and knowledge* and *acceptance and use of biometrics*) and *biometrics necessity.* Data collection and subsequent analysis shows that the engaged ministries face challenges of biometrics equipment miss-use and employees avoid or by pass the use of biometrics where possible. This could be attributed to the fact that most ministries pay little or no attention to equipping employees with the necessary technical skills such that they can appreciate and operate biometrics systems hence the need for making provisions on biometrics technical skills training. For example, the government of Andhra Pradesh, India, conducted workshops lasting at most one week, training its several agents who were identified for the implementation and use of a biometrics payment system which started in 2007. In addition, another way of promoting biometrics skills is through adding biometrics courses or programs in the education curriculum. For instance, educational institutions and organizations in the US launched new offerings and increased the frequency of existing short courses on biometrics with the aim of meeting the training needs in the field of biometrics technologies. All these efforts by several governments to promote technical biometrics skills affirm multimodal biometrics skills as a major component of biometrics implementation projects.

6.3.4 Social acceptance

To stimulate social acceptance, all stakeholders concerned have to be engaged in the deployment of biometrics. Numerous factors are seen as influencing the social acceptance of technology. For instance, the Unified Theory of Acceptance and Use of Technology identified four constructs, namely performance expectancy, effort expectancy, social influence and facilitating conditions, which are seen as direct determinants of user acceptance and usage behaviour (Venkatesh, Morris, Davis & Davis, 2003). As such, communities have to be engaged, making sure that they understand the rationale behind implementing biometrics systems. This can be done through outreach programs and workshops educating community members on biometrics and their role in their implementation and use. In addition, authorities responsible for promoting social acceptance can conduct pre-enrollment and enrollment awareness on the target audience. For instance, AADHAAR (2010) targeted influencers (e.g. teachers) in a society, educated them on biometrics and used them for spreading the message on biometrics. Additionally, the targeted audience is also provided with the necessary information during enrollment.

Another approach to promoting social acceptance is whereby the government can introduce educational programs on biometrics at different educational levels as done in the US (National Science and Technology Council, 2011). All these activities can have a positive impact on constructs that determine the social acceptance of biometrics.

6.3.5 Biometrics stakeholders

To achieve a successful implementation and use of biometrics systems, key stakeholders need to be identified and engaged in the project of biometrics. This attribute was derived from data collection and analysis. Data gathered to evaluate the impact of the political and governance aspects shows that *stakeholders* are critical players to the successful implementation of IT projects including biometrics implementations. The component of biometrics stakeholders implies the need to identify and include key stakeholders in the project, outlining their roles, indicating what is expected of them and also enquiring their views. The data collected and analysed shows that biometrics implementation in the Namibian government involves stakeholders summarized in Figure 13.

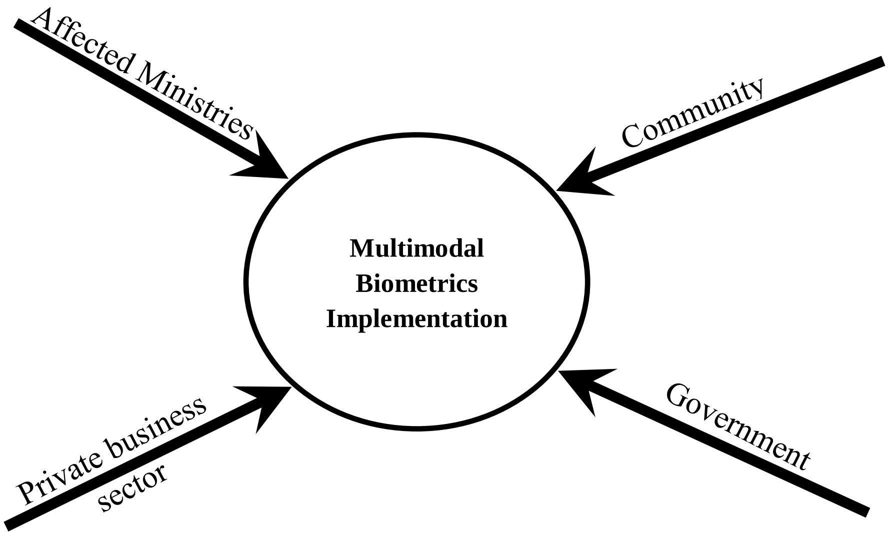


Figure 13: Stakeholders in the Namibian government biometrics implementation

- **Affected ministry or ministries** - this relates to the ministries that are involved in deploying biometric systems through their departments and divisions. Key members could include members of the respective IT Department, those that are to operate or use the biometrics. In addition, ministries can share resources for example, referencing to the same biometrics repository and as such they can also be identified as stakeholders.
- **The government** - through an Act of Parliament, the Namibian government establishes ministries which are in turn expected to perform certain mandates on behalf of the government. As the controlling authority, the government equips its ministries with technical, human and financial resources that they succeed in the conduct of their mandates. Accordingly, the government's contribution as a stakeholder is very critical to the success of biometrics implementation and use.

  The previous chapter showed how the Indian and US governments have been playing a pivotal role within their biometrics projects across different government departments and ministries.
- **Private businesses sector -** data collection and analysis shows that the business sector namely private companies like banks and insurance companies make use of instruments delivered by the government's biometric systems. For example, the business sector makes use of identification cards (issued by the Ministry of Home Affairs) with fingerprints and face or smart card with a memory chip that carries one's fingerprints, face, iris and some demographic information. For compatibility purposes, the business sector's views as stakeholders need to be considered.
- **The community -** the community plays the role of providing their biometrics traits for enrollment during the creation of such instruments like driver's licenses, and unique identification cards which are used for verification and authenticity purposes. However, certain issues that could affect the successful implementation of biometrics systems have to be addressed from the community's perspective. These can include issues to deal with ethical and health related concerns, and cultural biases. Jain and Kumar (2010) argue that these values are primarily concerned with privacy, trust, liberty, autonomy, equality, and informed consent that are widely perceived to be available to all the citizens in a democratic society.

6.3.6 Biometrics budget

The biometrics budget component was derived from one of the *biometrics challenges* that were raised through data collection and analysis: *biometrics costs*, as discussed in the previous chapter. Biometrics implementation involves a lot of issues that require sound financing such as the acquisition of the necessary biometrics technologies, training, research and development, crafting of polices and plans among other factors. For instance, the US government has invested a lot of funds in their biometrics technology projects through different government departments and divisions. For example, the US embarked on a project to implement the Next Generation Identification (NGI) system, replacing the Integrated Automated Fingerprint Identification System (IAFIS) in 2014 which has reached the end of its useful lifetime. The NGI system consits of an advanced matching algorithm with a search reliability of 99 percent compared to IAFIS' 95 percent. Such biometrics projects would require huge budgets to support research and development, implementation and training costs among other factors.

Due to huge budgets involved when dealing with biometrics systems, the biometrics budget is herein seen as one of the major components necessary for the success of biometrics technologies.

6.3.7 Biometrics polices, implementation standards and plans

The biometrics policies, implementation standards and plans component was derived from attributes of the technical aspects and the political and governance aspects. These include the availability of a *viable maintenance policy* at organisational level and biometrics *policies* at national level. In addition, properly laid out biometrics polices, implementation standards and plans are expected to partly address some of the biometric challenges, namely *failure to capture fingerprints* and *false rejection.* Previous studies and findings from Namibian ministries show that the successful implementation and use of biometrics require clearly drawn policies and plans at national and organizational or ministerial level. Interviewees highlighted the need for biometrics polices, with some of the policies still under crafting. As such, it could be that some of the challenges faced by the Namibian government on its implementation of biometrics could be solved through clearly drawn policies. In addition, constant evaluations and assessments of biometrics implementations are also necessary in order to evaluate if the implementation is being done according to the prescribed policies and guidelines. Some of the policies and implementation plans can focus on the following areas:

- Policy on standards for various biometrics attributes or biometrics traits to be used in the multimodal biometrics project such as using the face, fingerprints and iris. Besides the extent of biometrics traits' uniqueness and universality, Unar et al. (2014) noted that in terms of multiple attributes for multimodal biometrics, careful selection is the key point to success since selecting the modalities belonging to one region may not be a good choice because accidental loss of that organ will result in the user's inability to submit the required signature.
- Policy on the selection criteria for biometric technology to be used: a balance has to be stricken between quality and the cost of equipment. The performance or accuracy of a biometrics system is data dependent, usually influenced by environmental factors like temperature, humidity and illumination conditions around the system and performance factors such as capturing good quality images, composition of target user population, time interval between the enrolment and verification phases and robustness of recognition algorithms (Unar et al., 2014). The National Science and Technology Council (2011) has since identified different standards of biometrics products such as the Appendix F standard which has stringent image quality conditions, focusing on the human fingerprint comparison and facilitating large-scale machine one-to many matching operations (a system that compares one reference to many enrolled references) [NOT CLEAR FOR ME]. On the other hand a PIV-071006 is a lower-level standard designed to support 1:1 fingerprint verification.
- There has to be provisions to establish strict protocols for dealing with cases in which biometrics are impossible to use. Data collection and analysis reveals that there are instances where biometrics cannot work because an individual does not have the relevant infrastructure used for that particular biometrics system.
- Polices on biometrics and infants: Studies have shown that biometrics of children are not yet stabilized (UIDAI, 2010). To deal with this challenge, the government has to provide provisions on how toddlers and children's biometrics should be handled considering that children also deserve national identification documents. For example, in India, children's

biometrics are taken at around 5 years of age, and updated in the UID system every 5 years until the age of 18 (UIDAI, 2010). This will be enforced by an expiry date attached to the UID number, which will become invalid after that date (UIDAI, 2010).

- There is a need for a clear outline on the requirements for enrolment into the biometrics system. For instance, people can supply details like their name, address, age, gender, reference/witness and marital status during enrolment. This is necessary to ensure that the integrity and correctness of the data is not compromised while ensuring that the process of verification is non-harassing to individuals (UIDAI, 2010).
- Polices on legal, ethical and people's religions: One interviewee highlighted that religious and ethical issues can discourage people from accepting the use of biometrics. As such, polices have to be in place that cover privacy issues, ethical and health related concerns, and cultural biases (Jain & Kumar, 2010). These values are primarily concerned with privacy, trust, liberty, autonomy, equality and informed consent that is widely perceived to be available to all the citizens in a democracy (Jain & Kumar, 2010).

6.3.8 Biometrics trends and emerging technologies

This component interrelates with all other components. It focuses on new biometrics trends and emerging technologies and explores how these would affect the already identified components. Results from the Namibian participants reveal that quite often ministries have to replace old biometrics equipment with new equipment. This is consistent with the international trends, for instance, while most Namibian ministries considered for data collection are currently engaged in the implementation of AFIS, the US government considered replacing IAFIS in 2014 with the NGI because it has reached its useful lifetime and NGI is seen as much more efficient than AFIS, a clear result of emerging technologies in the biometrics field. In this regard, the National Science and Technology Council (2011) noted that research work has been done since 2006 to improve the architecture of biometrics technologies. These include studies focused on improving the biometrics modality performance and robustness, coming up with new algorithms, improving accuracy, designing databases with efficient indexing techniques for biometrics data and coming up with new biometrics traits and developing biometrics systems that can simultaneously acquire multiple modalities.

6.3.9 Biometrics consultants/committees

This component was identified through data collection analysis. Engaging biometrics consultants/committees is done to address biometrics challenges of a *lack of biometrics skills and knowledge* and attributes of *biometrics necessity* as discussed in the previous chapter. The data collected shows that not all ministries are acquainted with biometrics and their requirements. That is to say that the current shortage or lack of human resources with biometrics skills means that ministries will have challenges in identifying their biometrics needs that can suit their environment and associated tasks. As such, third parties with biometrics skills and some with the knowledge of uses for which the biometrics are to be used can be engaged so that they can carry out evaluations and recommend the best possible biometrics equipment to meet an organisation's needs. In addition, these committees or consultancies can also be set to advise on policy issues. This is consistent with international trends. For instance, the Indian government set up an independent committee for biometrics specialists to advise on the best biometrics traits to use in their biometrics user identification project.

6.3.10 Biometrics monitoring, evaluation and updating

In addition, biometrics implementation also requires a constant monitoring, analysis and evaluation to ensure that the whole implementation is going ahead smoothly and according to the prescribed policies. Biometrics monitoring will ensure that all unforeseeable challenges and issues are identified and reported to the responsible authorities. As already indicated in chapter 4 and 5, a number of concerns have been noted during and after biometrics implementation. For instance, one interviewee indicated that users often look for ways to override or avoid using biometrics technologies because they feel it is "*too much extra trouble".* Similarly, the government of Andhra Pradesh took a similar approach whereby it created a team responsible for monitoring progress, regularly interacting with stakeholders and flagging key issues, which has allowed the state to maintain a relatively high degree of visibility on the roll-out (Mukhopadhyay et al., 2013).

6.4 The framework for multimodal biometrics implementation

Figure 14 (next page) shows an outlay of the framework for multimodal biometrics implementation in Namibia. It is proposed that, for multimodal biometrics to be successfully implemented there is a need for clearly outlined **biometrics polices, implementation standards and plans.** All components are shown inside the oval of biometrics polices, implementation standards and plans, which implies that the overall multimodal biometrics implementation should be done within the realm of clearly drawn polices, implementation standards and plans.

It is also proposed that there is a need to identify the needed **multimodal ICT infrastructure** guided by the biometrics policies, implementation standards and plans for the successful implementation of multimodal biometrics. The size of the multimodal ICT infrastructure is big to emphasize the fact that this study's main focus as well as that of the model is on biometrics ICT infrastructure. The available multimodal ICT infrastructure enables the **biometrics architecture and technologies**. In other words, the available multimodal ICT infrastructure plays a major role in determining the biometrics architecture and technologies to be deployed, which in turn affects the needed **multimodal biometrics technical skills** that determine the successful implementation of multimodal biometrics. Even though multimodal ICT infrastructures are seen as enabling biometrics architectures and technologies, they also have a direct influence on the successful implementation of multimodal biometrics as shown by outward arrows directing to **multimodal biometrics implementation**.

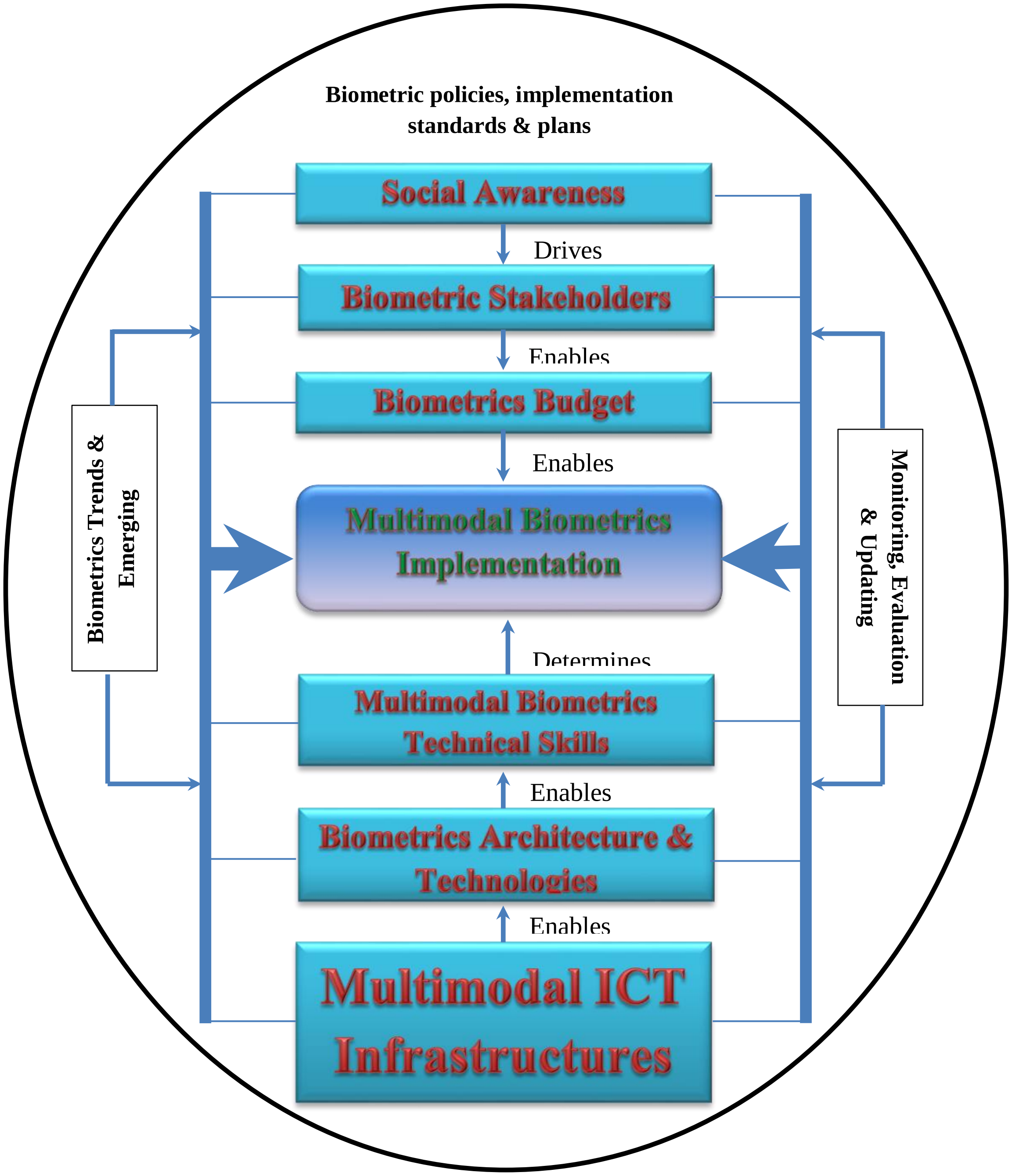

Biometric policies, implementation standards & plans
Social Awareness
Drives
Biometric Stakeholders
Enables
Biometrics Budget
Enables
Multimodal Biometrics Implementation
Determines
Multimodal Biometrics Technical Skills
Enables
Biometrics Architecture & Technologies
Enables
Multimodal ICT Infrastructures
Biometrics Trends & Emerging
Monitoring, Evaluation & Updating

Figure 14: Multimodal biometrics framework for the Namibia government

On the other side, **social acceptance** is seen as driving the extent of **biometric stakeholders**' involvement. In addition, biometrics stakeholders determine the **budget** to be allocated on biometrics projects, which has a direct effect on the successful implementation of multimodal biometrics. In addition, biometrics stakeholders' involvement and the enabling biometrics budget, social acceptance and biometric stakeholder involvement have a direct influence towards the successful implementation of multimodal biometrics. The collective influence of all these components is reflected by thick arrows pointing to multimodal biometrics implementation so as to emphasise the components' collective impact.

However, as the multimodal biometrics project moves on, it is necessary to constantly monitor, evaluate and update on such issues like progress or areas of concern with regards to multimodal ICT infrastructures, biometrics architecture and technologies, multimodal biometrics technical skills, social acceptance, biometrics stakeholders involvement, and biometrics budget. In addition, biometrics trends and emerging technologies are also seen as having an impact on the required multimodal ICT infrastructures, biometrics architecture and technologies and multimodal biometrics technical skills.

Similarly, biometrics trends and emerging technologies are seen as influencing social acceptance, biometrics stakeholder involvement and the needed biometrics budget to acquire the technologies.

6.5 Conclusion

The chapter looked at the rationale behind designing multimodal biometrics framework for the Namibian government. The lack of current frameworks on biometrics implementation motivated the designing of a framework for biometrics implementation in Namibia. The process of designing a framework for biometrics implementation involved a review of the current literature, engagement of the Namibian government through data collection, summarizing of findings comparing with current literature and the identification of major components. The identified components for the multimodal biometrics framework include: the ICT infrastructure; biometrics architecture and technologies; multimodal biometrics technical skills; social acceptance; biometrics stakeholders; biometrics budget; monitoring, evaluation and updating; biometrics trends and emerging technologies; biometrics policies, implementation standards and plans. The proposed framework concedes that, if biometrics deployments are to be successful in the Namibian government, these components have to be looked into. However, the whole process of biometrics deployment is to start with the outlining of the necessary biometrics policies, implementation standards and plans in such a way that all the other components will be looked into within the realm of these biometrics policies, implementation standards and plans.

CHAPTER 7: RESEARCH SUMMARY, RECOMMENDATIONS AND CONCLUSION

This chapter concludes the research by revisiting the research question and sub-questions and explaining what was done to address them.

7.0 Introduction

This thesis researched on multimodal biometrics with the aim of designing multimodal biometrics framework for the Namibian government. Through Chapter 2, the research explored the literature to establish priori constructs on biometrics technologies and implementations. Chapter 3 of this research explained how the data collection instrument was designed, the data collection process, analysis and all the precautions that were considered throughout these processes. It should be noted that there is limited literature on biometrics in Namibia and as such; the research used case studies from other countries on biometrics implementation and use to support findings from data collection. In addition, Chapter 6 of the study outlays the procedures followed in designing the framework for multimodal biometrics implementation in the Namibian government. Accordingly, this chapter concludes the research. The chapter revisits the proposed research questions and sub-questions of Chapter 1 and discusses what was done to meet the research question and sub-questions. This Chapter also gives an account of the research contributions and goes on to make propositions for future research areas.

7.1 Research question and summary of findings

Chapter 1 identifies the following statement as this research's main research question:

> *How should the Namibian government successfully prepare for multimodal biometrics deployment for different departments?*

Chapter 1 proposes the research's main objective as outlined below:

"Designing multimodal biometrics framework suitable for the Namibian government."

To meet the main objectives and address the main research question, the study design and proposes a framework for multimodal biometrics implementation in the Namibian government. The process and components of the proposed framework for multimodal biometrics implementation seek to address the research's sub-questions and respective sub-objectives. Accordingly, this section revisits the research question and sub-questions of Chapter 1 and gives an account on how these research questions were met.

The first research sub-question: *"How is the use of current biometrics in the Namibian context?"* was addressed through findings from data collection and analysis. It was found that, Namibian government departments use biometrics for controlling physical access to premises, accessing personal devices, accessing personal information and the verification of information. In addition, cross case analysis of Chapter 5 shows that the implementation and use of multimodal biometrics in Namibian governments is characterised by economical, technical, social and knowledge challenges. It was noted that multimodal biometrics are expensive, and as such the proposed framework for multimodal biometrics implementation identifies the biometrics budget as a major component of the framework that needs to be considered when implementing biometrics. Technical challenges with respect to interoperability, failure to capture fingerprints, false rejection and a lack of infrastructure were identified and addressed by components in the proposed framework. Issues to do with interoperability could be addressed through clearly drawn policies on careful selection criteria when purchasing biometrics technologies and engaging biometrics consultants/committees prior to purchasing. In addition, the proposed framework included the need for a police or plan that advises users on what to do in the event of the system's failure to capture fingerprints and false rejection. For example, alternative biometrics traits can be used if one trait is not working. Lastly, the proposed framework addressed the issues of ICT infrastructure by including ICT infrastructure as a component that has to be considered when implementing biometrics. In addition, challenges related to the acceptance and use of biometrics, lack of biometrics skills and knowledge were addressed through the social acceptance and multimodal biometrics technical skills components of the proposed framework. To enhance acceptance, it is considered that all stakeholders concerned be engaged. In addition, regular employee training on biometrics is seen as a solution to the lack of biometrics skills and knowledge.

The second research sub-question: "*What are the choices available to the government in terms of using multimodal biometrics technologies for security purpose?*" was addressed through the literature review of chapter 2 and data collected from the selected ministries. Chapter 2 outlined the criterion that qualifies biometrics traits namely universality, distinctiveness, invariance, collectability and performance. Accordingly, findings show that Namibian ministries use biometrics traits namely fingerprint, face, iris, signature, hand geometry and DNA.

The second research sub-question: *"What are the key multimodal biometrics technologies that work for different government departments?"* was met through data collection and analysis. The data collection instrument collected data on technologies used by ministries for their biometrics systems. It was found that different ministries have different needs that affect the choices of biometrics traits to be used. However, a common system that is used by most ministries is the AFIS system as the majority of ministries' biometrics systems are fingerprint based. In addition, the proposed framework for multimodal biometrics implementation included components namely the multimodal ICT infrastructure and biometrics architecture and technologies.

The third sub-question: *"What ICT infrastructure should be in place or is required to support multimodal biometrics deployment in Namibia?"* was met through data collection and analysis. Thus, through data collection and subsequent analysis, it was found that ICT infrastructures needed to support multimodal biometrics include a reliable wide area computer network connecting all the departments and divisions involved, computer servers with database for storing templates, biometrics devices such as scanners and cameras, respective software that processes biometrics traits and electricity to power the infrastructure (Mukhopadhyay et al., 2013; National Science and Technology Council, 2011; UIDAI, 2010; Unar et al., 2014). Consequently, ICT infrastructures are included in the proposed framework of multimodal biometrics implementation as one of the critical components that have to be looked at in order for a successful implementation of biometrics in Namibia.

7.2 The framework for multimodal biometrics implementation

The aim of this research was to design multimodal biometrics framework for the Namibian government. The framework is expected to give a guideline to the Namibian government in successfully preparing for multimodal biometrics deployments for different departments. Accordingly, the research was guided by the technology roadmap theoretical framework extracted from Jere et al. (2012) in designing the data collection instrument that was used to collect data from which the components of the framework were designed. The proposed framework for multimodal biometrics implementation concedes that for a successful biometrics implementation, there are major components that need to be looked into. These components include the ICT infrastructure; biometrics architecture and technologies; multimodal biometrics technical skills; social acceptance; biometrics stakeholders; biometrics budget; monitoring, evaluation and updating; and biometrics trends and emerging technologies. The consideration of these components is to be done within the spectrum of biometrics policies, implementation standards and plans. As such, it is argued that for a successful multimodal biometrics implementation, it is important that the whole implementation process starts with a clear outline of the biometric policies, implementation standards and plans. The other components will be looked into once there is a clear outline on the policies, standards and plans.

7.3 Research contributions and overall implications

The research found a number of factors that affect multimodal biometrics implementation in Namibia as articulated in Chapter 5. Even though the majority of these factors are comparable to the literature, this study went on to design a framework of multimodal biometrics implementation in Namibian government. By proposing a framework of multimodal biometrics implementations, the research does not only identify factors associated with biometrics implementation, rather, it went on to identify the components that are critical to the successful implementation of biometrics. The framework also shows how these components interrelate and how they should be approached in order to address issues of biometrics implementations, among them the associated challenges. In addition, the study also made the following contributions:

- Identifying the need for multimodal biometrics for the Namibian government. Data collection and analysis shows that, ministries recognize the need for biometrics. It was noted that as the population increases with new mechanisms being invented to breach the current security measures, biometric securities are some of the security measures that governments can consider for controlling physical access to its premises, accessing personal devices, accessing personal information and the verification of information.

- Producing a detailed step by step plan and reference document for multimodal biometrics deployment is another critical component. By proposing a framework of multimodal biometrics implementation for the Namibian government, the study gave a blue print that can be used as a source of guidance when implementing biometrics securities. In addition, the framework could be used for conducting audits whereby the framework would be used to assess if current biometrics implementations are taking into account all the major components that have to be considered for a successful biometrics implementation.
- Identifying biometrics technologies and related applications for government departments is yet another critical contribution. Whilst government departments have different needs, this study managed to identify different biometrics technologies and related applications for different departments. For instance, AFIS is one of the technologies used by the majority of ministries engaged. Such information can be used to ascertain the feasibility of using a single biometrics repertory from which all the ministries can be connected to.
- Identifying the ICT infrastructure to support the biometrics deployment in Namibia. The study also identified the necessary infrastructure to support biometrics deployment within the context of Namibia. This is important because research on case studies concedes that findings from one case are not easily transferable to another case as different contextual issues might affect its generalizability. Similarly, this was noted as the US government proposed to migrate from their biometric system AFIS to NGI in 2014, which is considered more efficient, while some of the Namibian ministries are currently implementing AFIS.
- Identify the challenges involved in implementing multimodal biometrics as opposed to unimodal biometrics. The study identified challenges that are specific to the Namibian government's project of biometric implementation as outlined in section 7.1.

7.4 Direction for future research

To further the study on multimodal biometrics implementations the following research areas could be considered:

- It is worthy researching on the feasibility of having a decentralised biometrics system with a network that is connected to relevant ministries, government departments and the private sector to promote consistency and the sharing of resources. For instance, such a system can link up with hospitals, immigration and assist with the individual identification. One such notable case is the case of India's biometrics unique identification project.
- There is also a need for further research on biometrics policies at government and organisational level. While this study identified relevant biometrics policies necessary for biometrics implementation and use, further research in this area needs to be done to come up with detailed policies that can guide the implementation and use of biometrics.
- The proposed framework of multimodal biometrics implementation can be used for studying the implementation of biometrics by governments in other developing countries. It may be worth examining whether the framework can be applied to the context of other developing countries in general. Such empirical attempts may enable researchers to extend the generalisability of the proposed framework of multimodal biometrics implementation.

7.5 Research conclusion

Governments in developing countries are keen on advancing with emerging security technologies, among them multimodal biometrics. Biometrics securities rely on using human physical body parts hence they cannot be lost and be forgotten among other advantages. Nevertheless, the subject of biometrics securities remain new to most governments in developing countries. As such, governments are faced with a number of challenges in implementing and ensuring a continued use of these biometrics securities. Accordingly, this study focused on designing multimodal biometrics framework for the Namibian government.

To arrive at the framework of multimodal biometrics implementation, firstly, a literature review was conducted to identify different biometrics traits and technologies that can be used in a biometrics security system. A review of case studies on uses of biometrics showed that biometrics securities are also becoming popular within government departments. In addition, the study was guided by Jere et al.'s (2012) technology roadmap theoretical framework in identifying the aspects that need to be looked into when implementing technologies. In particular, the technology roadmap theoretical framework was used for designing the questionnaire and interview questions of the data gathering instrument. The gathered data was analyzed through within and cross case analysis. Coding was used for case analysis. A framework of multimodal biometrics implementation in the Namibian government was derived from findings of data analysis. The framework was designed in part with the view of addressing challenges and other factors affecting biometrics implementation in Namibia. The framework comprises of components that one has to look at first in order to successfully implement multimodal biometric technologies. These components include Multimodal ICT Infrastructures; Biometrics Architecture and Technologies; Multimodal Biometrics Technical Skills; Biometrics policies, implementation standards and plans; Biometrics Trends and Emerging Technologies; Monitoring, Evaluation and Updating; Monitoring, Evaluation and Updating; Biometrics Budget; Biometric Stakeholders and Social Acceptance.

The proposed framework of multimodal biometrics implementation provides a step by step plan and reference document for guiding multimodal biometrics deployment.

REFERENCES

AADHAAR, (2010). AADHAAR - Communicating to a billion. Awareness and Communication Report. Published report: Unique Identification Authority of India (UIDAI) Planning Commission, Government of India. India, New Delphi.

Alshawi, S., Missi, F., & Irani, Z. (2011). Organisational, technical and data quality factors in CRM adoption - SMEs perspective. Industrial Marketing Management, 40:376–383.

Asmuni, H., Sim, M., Hassan, R. and Othman, R. M. (2014). Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images. Expert Systems with Applications.41:5390–5404.

Barde, S., Khobragade, S. & Singh, R. (2012). Authentication Progression through Multimodal Biometric System. International Journal of Engineering and Innovative Technology (IJEIT), 2(3):255-258.

Beranek, B. (2013). Voice biometrics: success stories, success factors and what's next. Biometric Technology Today

Beverland, M. B, Ewing, M. T. & Matanda, M. J. (2006). Driving-market or market-driven? A case study analysis of the new product development practices of Chinese business-to-business firms. Industrial Marketing Management, 35: 383–393.

Beverland, M., & Lindgreen, A. (2010). What makes a good case study? A positivist review of qualitative case research published in Industrial Marketing Management, 1971–2006. *Industrial Marketing Management, 39,* 56–63.

Bours, P. (2012). Continuous keystroke dynamics: A different perspective towards biometric evaluation. *Information Security Technical Report.* 17: 36 -43.

Canuto, A. M. P., Pintro, F. and Xavier-Junior, J. C. 2013. Investigating fusion approaches in multi-biometric cancellable recognition. Expert Systems with Applications. 40 :1971–1980

Cho, S. and Wang, S. (2006). Artificial Rhythms and Cues for Keystroke Dynamics based Authe ntication. *Proceedings of the International Conference on Biometrics, 5-7 January 2006, Hong Kong*.

Cho, S., Hwang, S. and Park, S. (2009). Keystroke dynamics-based authentication for mobile dev ices. *Computers & Security*. 28:85–93.

Clodfelter, R. (2010). Biometric technology in retailing: Will consumers accept fingerprint authentication? Journal of Retailing and Consumer Services. 17:181–188.

Collis, J. & Hussey, R. (2009). *Business Research: A practical guide for undergraduate & postgraduate students.* (3rd ed.). China: Palgrave Macmillan.

Connie, T., Jin, A. T. B., Ong, M. G. K. & Ling, D. N. C. (2005). An automated palmprint recognition system. Image and Vision Computing, 23(5):501-515.

Darvaes, J.R. (2010). Fraud Manual, Internal controls and fraud, Understanding employee embezzlement in the workplace. Available online at: http://www.fraud-examimers.org/fraud_manual.pdf

Dube, L. & Pare, G. (2003). Rigor in Information Systems Positivist Case Research: current Practices, Trends and Recommendations. *MIS Quarterly*, *27 (4),* 597-636.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory Building from Cases: Opportunities and Challenges. *Academy of Management Journal, 50 (1),* 25-32.

Ennis, J. and Nixdorf, W. 2012. Swapping PINs for palms – the potential of biometric technology in retail banking. Biometric Technology Today

FBI, (2011). Palm Print Recognition. National Science and Technology Council, Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics. Available online [Last Accessed 24/8/15]:http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/palm-print-recognition.pdf

Gold, (2013). Healthcare biometrics: solving the staff and patient security governance challenge. Biometric Technology Today http://biometrics.nist.gov/cs_links/pact/SSFS_113005.pdf

IT governance Institute (2004). Risk and Control of Biometric Technologies. A Security, Audit and Control Primer. *IT Governance Institute, Rolling Meadows, USA.*

Jain, A. K. & Kumar, A. (2010). Biometrics of Next Generation: An Overview. Second Generation Biometrics.

Jain, A. K., Ross, A. & Prabhakar, S. (2004). An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1):4-20.

Jamil, D. & Muhammad, A. K. (2011). Keystroke pattern recognition preventing online fraud. Available online at: http://www.Connections.ebscohost.com/c/articles/66134831/keystroke-pattern-recognition.

Jamil, D. and Muhammad, A.K. (2011). Keystroke pattern recognition preventing online fraud. Available oneline, accessed on 3/3/2013: http://www.Connections.ebscohost.com/c/articles/66134831/keystroke-pattern-recognition.

Jere, N. R., Thinyane, M. & Terzoli, A. (2012). A Methodological Framework for ICT Roadmap Development for Rural Areas. Published thesis-University of Fort Hare.

Kekre, H., B., Sarode, T, K, & Tirodkar, A., A. (2011). An Evaluation of Palm Print Recognition Techniques using DCT, Haar Transform and DCT Wavelets and Their Performance with Fractional Coefficients. *International Journal of Computer Applications. 32(1).*

Khitrov, M. (2013). Talking password: Voice biometrics for data access and security. *Biometrics technology today (2), 9-11.*

Kshetri, N. (2007). Barriers to e-Commerce and Competitive Business Models in Developing Countries: A Case Study. *e-Commerce Research and Applications, 6,* 443–452.

Kumar, A., Garg, S. & Hanmandlu, G. M. 2014. Biometric authentication using finger nail plates. *Expert Systems with Applications. 41:373–386.*

Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S., (2003). Handbook of fingerprint recognition. Springer-Verlag

Moses, K. R. (2011). Automated Fingerprint Identification System (AFIS). Unpublished Chapter. Available online: https://www.ncjrs.gov/pdffiles1/nij/225326.pdf

Mukhopadhyay, P., Muralidharan, K., Niehaus, P. and Sukhtankar, S. (2013). Implementing a Biometric Payment System: The Andhra Pradesh Experience. AP Smartcard Impact Evaluation Project. Policy Report

Mutelo R. (2014). Enhanced banking solution by Namibian biometric systems. Available at: http://www.newera.com.na/2014/09/17/enhanced-banking-solution-by-namibian-biometric-systems/

National Australian Bank, (2013). National Australian Bank: Major Bank implements Voice Biometrics and Call Steering Speech Recognition Solution. Available online: http://www.salmat.com.au/clients-case-studies/major-bank-implements-voice-biometrics-and-call-steering-speech-recognition-solution/

National Science and Technology Council (2011). The National Biometrics Challenge. National Science and Technology Council Subcommittee on Biometrics and Identity Management.

Ngcingwana, L. (2008). Eastern Cape Information and Communication Technology Strategy 2009-2014. Province of the Eastern Cape, Republic of South Africa.

Robert Wood Johnson Foundation (2008). Qualitative research guidelines. http://www.qualres.org/HomePosi-3515.html

Roux, L. l. (2005). Qualitative research: method in the madness? *A Working paper, University of Stellenbosch Business school*.

Salil, (2003). Biometric Recognition: Security and Privacy Concerns

Sathish, G., Saravanan, S. V., Narmadha, S. and Maheswari, U. (2012). Personal Authentication System using Hand Vein Biometric. *Int.J.Computer Technology & Applications. 3:383-391.*

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students* (5th ed.). New York: FT/Prentice Hall.

Seng, W. C., Unar, J. A. & Abbasi, A. (2014). A review of biometric technology along with trends and prospects. *Pattern Recognition. 47: 2673–2688.*

Sharma, Y. K., ShivaKumar, K. B., Srinidhi, G. A. & Kumar, M. J. (2014). Multi-Modality Biometric Assisted Smart Card Based Ration Distribution System. *International Journal of Application or Innovation in Engineering & Management (IJAIEM).* 3(6), 382-392.

Singh, M., Molla, A., Karanasios, S. and Sargent, J. (2008). Exploring the Impact of Government ICT Initiatives on the Livelihood of Australian Rural Communities. *BLED 2008 Proceedings.*

Smart Card Alliance, (2011). A Smart Card Alliance Physical Access Council White Paper. Available online. Last accessed 10/5/2015: http://irisid.com/download/news/Smart_Cards_and_Biometrics_030111.pdf

Solayappan, N. & Latifi, S. (2006). A Survey of Unimodal Biometric Methods. Proceedings of the 2006 International Conference on Security & Management, SAM 2006, Las Vegas, Nevada, USA, June 26-29.

South African Financial Intelligence Centre, (2012). Combating Financial Crime In South Africa Typologies Report.

Stier, K. (2011). IrisGuard Makes Inroads, from Mideast Banks to U.S. Prisons. BLOOMBERG L.P.

Sumalatha, K. A. and Harsha, H. (2014). International Journal of Advanced Research in Computer Science and Software Engineering. *International Journal of Advanced Research in Computer Science and Software Engineering. 4: 429-433.*

UIDAI, (2010). UIDAI Strategy Overview Creating a Unique Identity Number for Every Resident in India. *Unique Identification Authority of India (UIDAI) Planning Commission, Govt. of India*

UIDAI, (2011). Aadhaar. Security Policy & Framework for UIDAI Authentication Version 1.0. *Unique Identification Authority of India, India.*

Unar, J.A., Seng, W.C. and Abbasi, A. (2014). A review of biometric technology along with trends and prospects. *Pattern Recognition, 47, 2673–2688.*

Venkatesh, V. Morris, M., G. Davis, G., B., & Davis, D., F. 2003. User acceptance of information technology: toward a unified view. *MIS Quarterly*, *2,* 425-478.

Venkatraman, S., & Delpachitra, I. (2008). Biometrics in banking security: a case study. Information Management & Computer Security, 16(4), 415-430.

Wasserman, P. D. (2005). Solid State Fingerprint Scanners. A Survey of Technologies. Unpublished document. Available online:

William, (2001). Using Open Robust Design Models to Estimate Temporary Emigration from Capture-Recapture Data; Rhema Bjorkland Biometrics, 57(4):1113-1122.

Yadav, V. (2013). Unique Identification Project for 1.2 billion People in India. *Can it fill Institutional Voids and enable 'Inclusive' Innovation?* South Asia Institute (SAI) at Harvard University: Working Paper.

Yin, K. R. (2003). *Case Study Research: Design Methods* (3rd ed.). Thousand Oaks, Califonia: SAGE.

Zelazny, F. (2012). The Evolution of India's UID Program Lessons Learned and Implications for Other Developing Countries. *Center for Global Development, Washington DC, USA.*

APPENDIX A: A Full Schedule of the Interview Questions Used For Data Collection.

1. Describe your IT plan and indicate how it supports biometrics deployments
2. Do you have supporting IT infrastructure for biometrics
3. May you please brief me on the biometric securities you have implemented or you intend to implements?
4. What are the challenges you are encountering to fully implement biometrics?
5. How do you strategies the implementation of your biometrics for example do you have a policy, a plan that you follow? (Yes/No) what are the steps?
6. May you please outline who are the key stakeholders involved in the project of biometric security?
    a. What is the role of each one of them?
    b. Do you get necessary support for your IT plans from stakeholders or the government- suppose the government is a stakeholder?
7. Do you make any input/contributions or suggestions on the requirements of biometrics security within your division?
    a. If yes, please explain on the kind of input you give?
8. Do you feel these biometric technologies are necessary? And which ones do you prefer most?
9. Do you have an IT maintenance policy in place?
    a. How often do you do these routine checks?

APPENDIX B: A Full Schedule of the Questionnaire Used For Data Collection.

POLYTECHNIC OF NAMIBIA
SCHOOL OF COMPUTING AND INFORMATICS
Private Bag 13388 | 13 Stock Street | Windhoek, NAMIBIA
Tel: (+264 - 61) 207 – 2052 | Fax: (264 – 61) 207 – 9052
http://sit.polytechnic.edu.na /
Technology

transforming into
Namibia
University of
Science and

Name of Project – Development of a Multimodal Biometric Framework for the Namibian government

Dear Participant

The following questionnaire is part of Masters' research on **Development of a Multimodal Biometric Framework for the Namibian government**.

All information will be treated as ***Strictly Anonymity*** and will only be used for academic purposes. If you have any queries concerning the questionnaire, please contact the researcher whose contact details are set out below.

Researcher: Licky Richard Erastus

Cell: + 264 811281015

Fax: +264 61 218150

Email: s200516450@polytechnic.edu.na

Information about the Research

This research aims to develop a comprehensive framework for implementing multimodal biometric technologies that is suitable for Namibian government departments. To achieve this we have identified you to participate in this research.

The Testing Process

Data collection process will strictly adhere to permission given in the study consent form.

Participation and Confidentiality

Your participation in this research is completely voluntary and you have the right to withdraw at any time. No negative consequences will follow from withdrawal of participation in the research.

Please note that any data (*or images*) collected up to the point of withdrawal may be used within the study. Your ward will be supervised at all times by teacher/researcher. No personal information about you or your organizational details will be stored except information on the Department Name. Any information collected from this research will remain confidential and will be used for a Master of Science thesis project and scientific publications. In the documentation of our work, a pseudonym will be used (instead of the given names) for identification purposes. Information that would make it possible to identify a participant will never be included in any sort of report, or disclosed outside the project, unless explicit permission has been given.

Instructions for completion:

1. Please answer the questions as objectively and honestly as possible according to the instructions contained in the body of the questionnaire.
2. Please answer all the questions to allow an accurate analysis and interpretation of the data.

If you agree to the terms and references above, kindly take a while and complete the following questions.

1. **Have you ever heard of the term biometrics? Tick appropriate**

   Yes □

   No □

2. **Tick the type of biometrics you are aware of?**

   □ Fingerprint

   □ Face

   □ Iris

   □ Voice

   □ Signature

   □ Hand Geometry

   □ DNA

   □ Key stroke

3. **From the above list, state the ones you are using or you wish to use?**

a) ………………………………………………………………………………….

b) …………………………………………………………………………………….

c) …………………………………………………………………………………….

d) ………………………………………………………………………………………

4. What combination of biometrics do you prefer to use, from the list in nr. 2?

………………………………………………………………………………………………
……………………….…………………………………………………………………….
…………………………………………….……………………………………………….
………………………………………………………………………….…………………
………………………………………………………………………………………………

5. Tick the services that you are using biometric for?

□ Controlling physical access to a building.

□ Accessing personal information

□ Accessing personal devices

□ Verification of information

□ Others –

Specify……………………………………………………………………………………..
………………………………………………………………………………………………
……………………………………………………………………………………………..

6. Write the common biometric challenges experienced within your ministry or department?

………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
……………………………………………………………..……………………………….
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
…………………………..………………………………………………………………….
………………………………………………………………………………………………
………………………………………………………………………………………………
……………………………………………………………………………………………..
………………………………………………………………………………………………
………………………………………………………………………………………………

……………………………………………………………………………………………
……………………………………………………………..

7. **Biometrics usage & deployment**

(Indicate by placing a tick your views on each of the following statement i.e. on a 5- point Likert scale) where 1 – strongly disagree, 2- Disagree, 3- Neutral, 4- Agree & 5- Strongly Agree

Biometrics usage and deployments	**Strongly Disagree** **(1)**	**Disagree** **(2)**	**Neutral** **(3)**	**Agree** **(4)**	**Strongly Agree** **(5)**
1. Biometrics usage can improve security & identification of users.	□	□	□	□	□
2. Unimodal biometrics are less reliable than multimodal	□	□	□	□	□
3. Unimodal biometrics face more challenges that multimodal	□	□	□	□	□
4. Multimodal biometrics can improve speed and accuracy of biometrics	□	□	□	□	□
5. Combining figure prints and facial image can improve security of Biometrics.	□	□	□	□	□
6. Combining different biometrics can improve usage.	□	□	□	□	□
7. Biometrics implementation requires large database space.	□	□	□	□	□
8. Biometrics technologies are expensive.	□	□	□	□	□
9. Biometrics deployments require a good budget	□	□	□	□	□
10. Biometrics technologies require regular updates.	□	□	□	□	□
11. Some users feel unsecure to use biometrics technologies.	□	□	□	□	□

12. Some users lack trust in using biometrics technologies.	□	□	□	□	□
13. Biometrics technologies require technical skills to all users.	□	□	□	□	□
14. Biometrics deployment requires training and regular refresh courses.	□	□	□	□	□
15. The user acceptance of using biometrics in Namibia is very low.	□	□	□	□	□
16. Biometrics are required in all public service departments.	□	□	□	□	□
17. Biometrics deployment requires proper National policies.	□	□	□	□	□
18. Biometrics stakeholders in Namibia are promoting deployments.	□	□	□	□	□
19. Biometrics stakeholders in Namibia are working together	□	□	□	□	□
20. Biometrics deployment require a well-planned ICT infrastructure	□	□	□	□	□
21. Biometrics deployments require stakeholders engagement	□	□	□	□	□
22. Biometrics deployment requires identification & use of appropriate technologies	□	□	□	□	□

APPENDIX C: THE FACULTY APROVAL

SCHOOL OF COMPUTING AND INFORMATICS

Research Topic: Designing a Multimodal Biometric Framework for the Namibian government.

This serves to confirm that Licky Richard Erastus: Cell: + 264 811281015: Fax: +264 61 218150: Email: s200516450@polytechnic.edu.na or licky001@gmail.com : is a Masters student within the Informatics Department. I would like to ask for your permission to involve your Ministry/Department in this research.

Interviews, observations and a questionnaire will be done to get information that will help in the Development of a Multimodal Biometric Framework for the Namibian government.

All information will be treated as confidential and will only be used for academic purposes. If you have any queries concerning the questionnaire, please contact the researcher whose contact details are set out above.

Information about the Research

This research aims to develop a comprehensive framework for implementing multimodal biometric technologies that is suitable for Namibian government departments. To achieve this we have identified you to participate in this research.

The Testing Process

Participation and Confidentiality

Your participation in this research is completely voluntary and you have the right to withdraw at any time. No negative consequences will follow from withdrawal of participation in the research.

Please note that any data (*or images*) collected up to the point of withdrawal may be used within the study. No personal information about you or your organizational details will be stored except information on the Department Name. Any information collected from this research will remain confidential and will be used for a Master of Science- Informatics thesis project and scientific publications. In the documentation of our work, a pseudonym will be used (instead of the given names) for identification purposes. Information that would make it possible to identify a participant will never be included in any sort of report, or disclosed outside the project, unless explicit permission has been given.

Further Questions and Contact Details

Data collection process will strictly adhere to permission given in the study consent form.

Dr Nobert Jere
Senior Lecturer - Polytechnic of Namibia
Department of Informatics (HOD)
Windhoek, Namibia
Office number: +264 61 207 2746
Mobile: +264 81 406 4683