We have credited your above account with

Kenya Shillings TWO THOUSAND ONLY

CASH PAID IN BY: DORCIS ARSHLEY SHILOKA
RESEARCH PERMIT ERH

Transaction Number: T717052K507 at 11:56:99 on 21/02/2017

Thank you for banking with us. You were served by NYUMBA JOHN AHANA

*** Advice not valid unless Transaction number is shown ***
A MODEL FOR ADOPTION OF MULTIMODAL BIOMETRIC SECURITY SYSTEMS IN PRIVATE ORGANIZATIONS

Dorcus Arshley Shisoka

A research proposal submitted in partial fulfillment for the requirements for the award of Doctor of Philosophy in Information Technology of Kibabii University

NOVEMBER, 2016
DECLARATION
This research proposal is my original work prepared with no other than the indicated sources and support and has not been presented elsewhere for a degree or any other award.

Signature: ___________________________ Date: 29/11/2016

Dercus Arshley Shisoka

PHD/IT/0004/13

APPROVAL
The undersigned certify that they have read and hereby recommend for acceptance of Kibabii University a research proposal entitled “A model for Adoption of Multimodal Biometric Security Systems in Private Organizations”

Signature: ___________________________ Date: 29/11/2016

Dr. Anselemo Peters Ikoha, PhD
Department of Information Technology
Kibabii University

Signature: ___________________________ Date: 29/11/2016

Prof. Franklin Wabwoba, PhD
Department of Information Technology
Kibabii University
ABSTRACT

Multimodal systems, which consolidate information from multiple biometric sources, are gaining popularity because they are able to combine a number of traits to be used in authentication unlike traditional conventional systems and uni-modal biometric security systems. However, many organizations today have adopted and use unimodal biometric security systems for authentication, but these unimodal biometric security systems have been found to be weak and vulnerable. These security systems lack accuracy, experience noisy sensor data and are susceptible to spoofing. This has led to limited adoption and lack of user acceptance of biometric technology let alone multimodal biometric security systems. This research seeks to investigate the current biometric security systems and develop a model for a multimodal biometric security system for identity verification in private organizations. This study intends to achieve this by determining the types of biometric security systems being used, measuring recognition performance of unimodal biometric security systems in private organizations, assessing the effectiveness of biometric security technologies being used in authentication security systems in organizations in Kenya and in turn developing a tool for assessing the level of adoption of multimodal biometric security systems by organizations. Mixed method research design will be employed in this study. This will consist of survey and experimentation. The study will be conducted in Nairobi, Kenya. The target population will comprise of private organizations. Purposive sampling will be used to identify one organization that has employed biometric technology use for authentication. Thereafter snowball sampling will be used to identify other organizations that use biometric technologies. Survey will employ questionnaires, interview and document analysis while experimental design will entail observations followed by prototyping. Data obtained from questionnaires will be analyzed using descriptive statistics to establish the meaning of the constructs under study. Data will also be subjected to inferential statistics involving Pearson Product Moment Correlation, factor analysis and statistical modeling. Prior to the study, permission and clearance will be sought from the relevant bodies. The output of this study will document the types of biometric security systems; assess the effectiveness of the biometric security technologies employed in authentication systems in these organizations. Consequently, this study will develop a tool to assess the level of adoption of multi modal biometric security systems by organizations. The findings of the study will inform organizations on the factors influencing the adoption of biometric security systems, provide useful knowledge for informed decisions and policies in procurement and adoption of biometric security systems, thus help to improve user acceptance of multimodal biometric security technology in these organizations hence enhance security.
TABLE OF CONTENTS

DECLARATION ........................................................................................................ vi
APPROVAL ............................................................................................................. vii
ABSTRACT .............................................................................................................. viii
LIST OF TABLES .................................................................................................... ix
LIST OF APPENDICES .......................................................................................... x
LIST OF FIGURES .................................................................................................. xi
DEFINITION OF OPERATIONAL TERMS .............................................................. xiii
ABBREVIATIONS AND ACRONYMS ..................................................................... xiv
CHAPTER ONE ...................................................................................................... 1
INTRODUCTION ...................................................................................................... 1
  1.1 Background of the study .................................................................................. 1
  1.2 Statement of the Problem ................................................................................ 4
  1.3 Purpose of the Study ....................................................................................... 4
  1.4 Objectives of the Study .................................................................................. 4
  1.5 Research Questions ......................................................................................... 5
  1.6 Scope of the Study .......................................................................................... 5
  1.7 Significance of the Study ................................................................................. 5
  1.8 Justification .................................................................................................... 6
  1.9 Limitations of the study .................................................................................. 6

CHAPTER TWO ...................................................................................................... 7
LITERATURE REVIEW ............................................................................................ 7
  2.1 Introduction to Literature Review .................................................................... 7
  2.2 Types of Biometric Security Systems in existence ........................................ 7
  2.2.1 Unimodal Biometric System ..................................................................... 9
  2.2.2 Multimodal Biometric System .................................................................. 12
  2.3 Biometric Security Technologies and their Effectiveness .............................. 12
  2.3.1 Signature Dynamics .................................................................................. 16
  2.3.2 Fingerprint Recognition .......................................................................... 17
  2.3.3 Iris Recognition ....................................................................................... 18
  2.3.4 Facial-Scan Technology .......................................................................... 19
  2.3.5 Hand Geometry ....................................................................................... 20
  2.3.6 Retinal Scan ............................................................................................ 21
  2.3.7 Vascular Patterns .................................................................................... 22
LIST OF TABLES

Table 2.1: State-of-the-art error rates associated with fingerprint face and voice biometric systems ........................................................................................................................................50

Table 3.1: Data analysis procedure summary ........................................................................................................................................60
LIST OF APPENDICES
Appendix I – Questionnaire .................................................................72
Appendix II – Interview guide..............................................................77
Appendix III – Observation guide .........................................................81
Appendix IV – Schedule ..................................................................82
Appendix V – Budget ....................................................................83
LIST OF FIGURES

Figure 2.1 – Technology acceptance model.................................................................17

Figure 2.2 – Theory of reasoned action.................................................................18

Figure 2.3 – Components of TPB.............................................................................19

Figure 2.4 – Decomposed theory of planned behaviour......................................20

Figure 2.5 – Innovation diffusion model..............................................................21

Figure 2.6 – Technology, organization and environment framework....................22

Figure 2.7 – Unified theory of acceptance and use of technology model..............23

Figure 2.8 - Block Diagram of the Enrollment phase..............................................26

Figure 2.9 - Block Diagram of the Verification phase.............................................27

Figure 2.10 - Block Diagram of the Identification phase......................................27

Figure 2.11 – Block Diagram of General Biometric system.................................38

Figure 2.12 – Conceptual Framework.....................................................................41
DEFINITION OF OPERATIONAL TERMS

Adoption: The process used to determine whether or not to undertake an exercise or accept and use an innovation.

Biometrics: Refers to authentication technology that relies on measurable physical characteristics that can be automatically checked.

Biometric Authentication: Biometric authentication refers to automated methods of identifying or verifying the identity of a living person in real-time based on a physical characteristic or personal trait.

Biometric Security Systems: Information systems that use biometric authentication for access.

Enrolment: The process of adding users credentials to the authentication system.

Identification: The act of finding out who someone is or what something is.

Information and Communication Technology: It’s an umbrella term that includes any communication device and application.

Model: A simplified and idealized understanding or simulation of a physical system to replicate its behaviour.

Multimodal: Multimodal biometric systems utilize more than one physiological or behavioral characteristic for enrollment, verification, or identification.

Organization: A social unit of people that is structured and managed to meet the need or pursue collective goals.

Security Systems: A Computer system protected through the use of special hardware, software, policies and practices against data corruption.

Unimodal: Unimodal biometric system depends on the single source of Information, physiological or behavioral characteristic for enrollment, verification, or identification.

Recognition: The act of accepting that something is true or important or that it really exists.

Verification: The process of establishing the truth, accuracy or validity of something.

Noise: Is unwanted electrical or electromagnetic energy that degrades the quality of signals and data.
### ABBREVIATIONS AND ACRONYMS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATB</td>
<td>Attitude Towards Behaviour</td>
</tr>
<tr>
<td>ATM</td>
<td>Automated Teller Machine</td>
</tr>
<tr>
<td>BSEM</td>
<td>Bayesian Statistical Equation Modelling</td>
</tr>
<tr>
<td>BSS</td>
<td>Biometric Security Systems</td>
</tr>
<tr>
<td>BST</td>
<td>Biometric Security Technologies</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed Circuit Television</td>
</tr>
<tr>
<td>DOI</td>
<td>Diffusion of Information</td>
</tr>
<tr>
<td>DOS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DVD</td>
<td>Digital Versatile Disks</td>
</tr>
<tr>
<td>EAC</td>
<td>Electronic Access Control</td>
</tr>
<tr>
<td>EDI</td>
<td>Electronic Data Interchange</td>
</tr>
<tr>
<td>ERP</td>
<td>Enterprise Resource Planning</td>
</tr>
<tr>
<td>FRVT</td>
<td>Face Recognition Vendor Test</td>
</tr>
<tr>
<td>FpVTE</td>
<td>Fingerprint Vendor Technology Evaluation</td>
</tr>
<tr>
<td>FVC</td>
<td>Fingerprint Verification Competition</td>
</tr>
<tr>
<td>HIS</td>
<td>Health Information System</td>
</tr>
<tr>
<td>HMN</td>
<td>Health Metrics Network</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>ID</td>
<td>Identity Card</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IS</td>
<td>Information Systems</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>LIS</td>
<td>Library Information System</td>
</tr>
<tr>
<td>MBSS</td>
<td>Multimodal Biometric Security Systems</td>
</tr>
<tr>
<td>MCMC</td>
<td>Markov Chain Monte Carlo</td>
</tr>
<tr>
<td>NACOSTI</td>
<td>National Commission of Science, Technology and Innovation</td>
</tr>
<tr>
<td>NIST</td>
<td>The National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OSCE</td>
<td>Organization for Security and Cooperation in Europe</td>
</tr>
<tr>
<td>PBC</td>
<td>Perceived Behaviour Control</td>
</tr>
<tr>
<td>PERM</td>
<td>Perceived E-readiness Model</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>SGS</td>
<td>School of Graduate Studies</td>
</tr>
<tr>
<td>SN</td>
<td>Subject Norm</td>
</tr>
<tr>
<td>TAM</td>
<td>Theory of Acceptance Model</td>
</tr>
<tr>
<td>TPB</td>
<td>Theory of Planned Behavior</td>
</tr>
<tr>
<td>UBSS</td>
<td>Unimodal Biometric Security System</td>
</tr>
</tbody>
</table>
CHAPTER ONE

INTRODUCTION

1.1 Background of the study

Human beings have been recognizing each other according to various characteristics for ages. We recognize others by their face when we meet them and their voice as we speak to them. Authentication in computer systems has been traditionally based on something that one has for example a key, chip card or identity card which they carry around or something that one knows such as a Personal Identification Number (PIN). However things like or cards tend to get stolen or lost while passwords can be forgotten or often disclosed. To achieve maximum security a more reliable identification and verification of the individual should be done. This should use something that really characterizes the individual. By contrast to possession based (what we own such as a key) or knowledge-based (what we know such as password), biometrics is based on what we are and how we behave.

Biometric authentication refers to automated methods of identifying or verifying the identity of a living person in real time based on a physical characteristic or personal trait (Tripathi, 2011). The phrase “living Person” in real time is used to distinguish biometric authentication from forensics, which does not involve real time identification of a living individual. Biometrics is essentially, based on the development of pattern recognition systems. Today, electronic or optical sensors such as cameras and scanning devices are used to capture images, recordings or measurements of a person’s unique characteristic (Drosou et al, 2015).

Due to these developments biometric identification has eventually acquired a much broader relevance today because the computer interface has become more natural. It’s an automated method of recognizing a person based on their physiological or behavioral characteristics. A physiological characteristic is relatively a stable human physical characteristic such as fingerprint, iris pattern, facial geometry and hand geometry. On the other hand, a behavioral characteristic is a reflection of an individual’s psychological
The digital data captured from the individual is then encoded and can be stored and searched on demand through a computer. Such biometric search is not only rapid it is also a process that is accepted globally in establishing forensic evidence. Consequently there are numerous forms of biometrics now being built into technology platforms. However the adoption of biometric technology is relatively slow because this technology is new and as such has not fully matured (Allan & Ouellet, 2006; Tripton & Krause, 2008). This immaturity is not only limited to the technology itself, but extends to other areas such as legislation, standards and governance resulting in challenges relating on interoperability, usability and acceptance (Grother & Phillips, 2006). This acceptance has also affected the rate of adoption of Biometric Security Systems (BSS) by organizations in Kenya.

Most organizations in Kenya have adopted biometric systems that use only one trait or a combination of only two traits for authentication otherwise known as unimodal biometric system. The systems adopted use an identity card photograph and signature or a photograph representation and fingerprint and Closed Circuit Television (CCTV). However, such BSS generally suffer from enrollment problems like non-universal biometric traits, are susceptible to biometric spoofing and experience insufficient accuracy caused by noisy data acquisition in certain environments (Moody, 2004). Because of these weaknesses organizations have continued to suffer from instances like transaction fraud, impersonation, phishing, man in the middle (MITM), brute force, spyware and social engineering.

Unimodal biometric system depends on the single source of information, physiological or behavioral characteristic for enrollment, verification, or identification. When a fingerprint biometric system is utilized as identification, then the system will match the fingerprints in the given database. A recent report by the National Institute of Standards and Technology (NIST) to the United States Congress concluded that approximately two percent of the population does not have a legible fingerprint and therefore cannot be enrolled into a fingerprint biometrics system (NIST, 2000).
Several other biometric systems have been developed earlier: biometric systems based on palm print and hand geometry features has been developed (Kumar & Shekhar, 2010; Ribaric & Fratric, 2006). However in such a system both the biometric features are acquired as image signals and hence may not provide robustness against noise. There have been biometric systems developed using face; fingerprint and hand geometry features (Jain & Ross, 2002). Unfortunately such systems also suffer from the same limitation mentioned above. These limitations of unimodal biometric system are positively overcome with use of multiple source of information from the user, which also increases the security of the system.

To overcome these problems organizations should adopt and use multimodal biometrics. Multimodal biometric systems utilize more than one physiological or behavioral characteristic for enrollment, verification, or identification. It can provide reliable and secure applications than unimodal biometric system due to multiple pieces of evidence (Kuncheva, 2004). In most of these systems the objective is to develop multimodal system using existing unimodal systems for improving the performance than that that can be achieved using any of the unimodal systems in the combination. Since the individual unimodal systems are from different biometric technologies the improvement can be achieved by combination.

Driven by lower hardware costs, a multimodal biometric security system uses multiple sensors for data acquisition. This allows capturing multiple samples of a single biometric trait (called multi-sample biometrics) and/or samples of multiple biometric traits (called multi source or multimodal biometrics). This approach also enables a user who does not possess a particular biometric identifier to still enroll and authenticate using other traits, thus eliminating the enrollment problems and making it universal (Tripathi, 2011).

This research therefore is designed to investigate the adoption of multimodal BSS and develop a working model for organizations. The model will attempt to provide improved security in the current unimodal systems being used by organizations.
1.2 Statement of the Problem

Biometric Security Systems are slowly creeping into the information systems world and taking over the traditional systems (Ayana, 2014). This is because they employ the use of physiological or behavioural characteristics for authentication. As the level of automation goes high due to improved technology, security breaches and transaction, fraud increases (Drosou et al, 2015). Therefore there is need for adoption of a highly secure identification and personal verification technology. Until today organizations have implemented and used unimodal BSS whose authentication and identification methods include the use of only one biometric trait. Not only have these been found to be weak methods for securing an organization but such systems suffer from lack of accuracy, limitation in enrollment rates, and susceptibility to spoofing (Rane et al, 2013). In the end such systems are vulnerable and have on a number of occasions been by-passed by external forces. Multimodal Biometric Security Systems (MBSS) that utilize more than one physiological and behavioural characteristic for enrollment are now gaining popularity because they are able to overcome most limitations experienced by unimodal authentication systems. Although such technologies exist, most organizations are yet to adopt them. To improve the security of resources in organizations this research seeks to investigate the performance of existing biometric security systems and develop a model for adoption of multi modal biometric security systems.

1.3 Purpose of the Study

The purpose of this study is to investigate the performance of existing biometric security systems being used in private organizations in Kenya and thereafter develop a model for adoption of MBSS by private organizations.

1.4 Objectives of the Study

The objectives of this study are to:-

i. Determine the biometric security systems being used in private organizations.

ii. Assess the effectiveness of the existing biometric security technologies used in authentication security systems in private organizations.

iii. Measure recognition performance of unimodal biometric security systems in private organizations.
iv. Develop a tool to assess the level of adoption of multimodal biometric security systems by organizations

1.5 Research Questions
i. What biometric security systems are currently in use by private organizations?
ii. How effective are the existing biometric security technologies in authentication security systems in private organizations?
iii. What is the recognition performance of unimodal biometric security systems in private organizations?
iv. How does the developed tool assess the level of adoption of multimodal biometric security system?

1.6 Scope of the Study
The study will focus on biometric security systems used in private organizations. These organizations are chosen because that is where the data to be used in the study can be found. The study will be carried out in Nairobi city in Kenya. This city has been chosen because of its infrastructure as well as it being a security hub. The study will be conducted in organizations that have already adopted biometric technologies to investigate their performance and not the hardware or software components. Because of the various areas to be studied this research work will collect both qualitative and quantitative data. This study will be conducted within two years.

1.7 Significance of the Study
i. This study is expected to provide a basis for extension of knowledge on Multimodal Biometric Security Systems on their use in various private organizations in Kenya.
ii. The study will also improve user acceptance of new technology by demystifying how this new technology is implemented and diffused.
iii. The output of this study will provide useful knowledge for informed decisions and policies in procurement and adoption of biometric security systems.
iv. The outcome of this study is expected to improve the adoption of multimodal biometric security systems hence enhance security in organizations
1.8 Justification

Insecurity is a common problem, not only to the government but it has encroached into private organizations as well. There have been reported cases of impersonation where an individual can pass on as someone else. On such occasions, these fraudsters have been able to access information or property that does not legally belong to them. The reason as to why insecurity is escalating is the type of identification and verification methods employed by these organizations for use in their authentication security systems (Gupta, 2011).

The use of unimodal biometric identification methods presents a relatively weak security system that can easily be by-passed. This is the reason for carrying out this research on adoption of multimodal biometric security system as this will enable most organizations to protect their resources and information by combining the features of unimodal biometric technologies. The findings of the study on the relative weaknesses of the unimodal systems will inform the stakeholders so as to make better decisions on matters of security. These findings will also provide a benchmark for use of multimodal biometric security systems as a tool for identification and authentication in organizations in Kenya.

The model to be created will add value to the existing biometric security models and enhance data security in most organizations in Kenya. By obtaining this doctorate the researcher will contribute to the nation’s development as a resource person which will in turn contribute to the realization of Kenya’s vision 2030 and sustainable development.

1.9 Limitations of the study

The research will be cautious in generalizing the findings to the entire population since the study will investigate only private organizations. This study adopts a one-time survey research; according to London school of hygiene and tropical medicine (2009) surveys conducted at only one point in time cannot reveal a strong evidence of cause-effect relation. This study utilizes snowball sampling technique which is a non-probability sampling technique. This technique inherently prevents generalization of findings to the wider population.
CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction to Literature Review
This chapter discusses the various types of biometric security systems. It elaborates on the various biometric security technologies as well as indicators of effectiveness of BST. It discusses measures of recognition performance of unimodal BSS. It also presents literature on some tools that have been developed to assess the levels of adoption of BSS. It further describes the theoretical framework that underpins this study. It also captures the research gaps informing this study and concludes by displaying the independent and dependent variables under study in a conceptual framework.

2.2 Types of Biometric Security Systems in existence
Security is the degree of resistance to, or protection from, harm (Pooe & Labuschagne, 2011). It applies to any vulnerable and valuable asset, such as a person, dwelling, community, item, nation, or organization. System security is a means or method by which something is secured through a system of interworking components and devices (Kreizman et al., 2007). The initial layer of security uses crime prevention through environmental design to deter threats. Some of the most common examples are also the most basic: warning signs or window stickers, fences, vehicle barriers, vehicle height-restrictors, restricted access points, security lighting and trenches.

According to the Kenyan e-Government Strategy (2004), one of the major reasons as to why organizations are utilizing Information and Communication Technology (ICT) is to improve security within the organization. However, as issues of insecurity become an area of concern, most organizations still experience problems like transaction fraud, access control, impersonation, social engineering and man in the middle, conmen as well as data leaks as a result of escalated insecurity. Technological advancements have made many organizations to shift from manual (or traditional) security `systems to electronic systems. In an effort to salvage themselves from these threats most organizations are making efforts to protect information they hold dear.
Traditional technologies used to authenticate individuals for logical access by various organizations in Kenya today include; password authentication, personal identification numbers and identity cards. These traditional technologies have their shortfalls. For instance, passwords have been widely recognized as a weak form of authentication with increasing amounts of password theft, either directly from the owner, through network intrusion, covert observation or unauthorized database access (Saba, 2012). Passwords can also be easily forgotten, guessed, hacked, stolen, shared or swapped (Hussain, 2016) which puts organizations in danger. Hussain (2016) observed that researchers at Verizon attributed 48% of data breaches involving hacking to stolen password. Therefore, passwords are considered rather obsolete and highly vulnerable.

On the other hand, PINs are not as secure as they can be disclosed or even forgotten. In such circumstances then the user is inconvenienced as they have to follow a set of procedures before they can acquire a new PIN and this interferes with their normal livelihood (Ravi, 1994). There are also rising concerns about identity theft and the misuse of public services, this has led to the doubt if really identity cards can be used to identify an individual wholly. However, it is clear that the ability to properly identify a person would prove challenging because these can be stolen and even falsified.

Biometrics is an emerging field of information technology which aims to automatically identify individuals using their unique biological traits. By measuring the physiological and behavioral characteristics using the individual’s biological samples, it has been shown that information characteristics of each individual can be extracted in order to verify the identity of the individual in a population. As such it identifies individuals by “who they are” which eliminates the need to remember passwords and PINs and prevent unauthorized access from others who may have the means to steal passwords. Biometrics is defined as the unique (personal) physical or logical trait of the human body. It is a study of automated methods for recognizing human beings based upon one or more parts of the human body or the behavior of the person.

According to Moody (2009), a biometric system is a system that uses physiological and/or behavioral characteristics of a human being to authenticate a system as verification and identification systems. Physiological characteristics provide the ability to control and to
protect the integrity of sensitive data stored in information systems. Behavioural biometrics is a measure that uniquely identifies and measures patterns in human activities and is used for secure authentication. Thus, the application of biometrics in security systems is able to secure online transactions and data stored electronically.

2.2.1 Unimodal Biometric Security System (UBSS)

Biometric identification systems which use a single biometric trait of the individual for identification and verification are called unimodal systems. A unimodal biometric security system (Ross & Jain, 2003) consists of three major modules: sensor module, feature extraction module and matching module. The performance of such a biometric system is largely affected by the reliability of the sensor used and the degrees of freedom offered by the features extracted from the sensed signal.

Unimodal biometric system depends on the single source of information, physiological or behavioral characteristic for enrollment, verification, or identification. Although unimodal biometric security systems might seem very proficient, in reality there are numerous challenges when enrolling large populations using just a single (unimodal) biometric trait? The major issue with unimodal biometric security systems is that no one technology can be suitable for all applications. Unimodal biometric systems have limitations in terms of accuracy, enrollment rates, and susceptibility to spoofing (Ross & Jam, 2001). The following are the limitations of unimodal biometric security systems:

(a) Noisy sensor data: Noise can be present in the acquired biometric data mainly due to defective or improperly maintained sensors. For example, accumulation of dirt or the residual remains on a fingerprint sensor can result in a noisy fingerprint image. Failure to focus the camera appropriately can lead to blurring in face and iris images. The recognition accuracy of a biometric system is highly sensitive to the quality of the biometric input and noisy data can result in a significant reduction in the accuracy of the biometric system (Chen et al., 2005).

(b) Non-universality: If every individual in the target population is able to present the biometric trait for recognition, then the trait is said to be universal.
Universality is one of the basic requirements for a biometric identifier. However, not all biometric traits are truly universal. The National Institute of Standards and Technology (NIST) has reported that it is not possible to obtain a good quality fingerprint from approximately two percent of the population (people with hand-related disabilities, manual workers with many cuts and bruises on their fingertips, and people with very oily or dry fingers) (NIST, 2015). Hence, such people cannot be enrolled in a fingerprint verification system.

Similarly, persons having long eye-lashes and those suffering from eye abnormalities or diseases like glaucoma, cataract, aniridia, and nystagmus cannot provide good quality iris images for automatic recognition (BBC News, 2016). Non-universality leads to Failure to Enroll (FTE) and/or Failure to Capture (FTC) errors in a biometric system. This tends to lock out some users from accessing the services being provided by the system and thus make the system not operate universally.

(c) Lack of individuality: Features extracted from biometric characteristics of different individuals can be quite similar. For example, appearance-based facial features that are commonly used in most of the current face recognition systems are found to have limited discrimination capability (Golfarell et al, 1997). A small proportion of the population can have nearly identical facial appearance due to genetic factors (e.g., father and son, identical twins, etc.). This lack of uniqueness increases the False Match Rate (FMR) of a biometric system, making the system to accept and allow the user to access the resources yet they are not the authentic user.

(d) Lack of invariant representation: The biometric data acquired from a user during verification will not be identical to the data used for generating the user’s template during enrollment. This is known as “intra-class variation”. The variations may be due to improper interaction of the user with the sensor (e.g., changes due to rotation, translation and applied pressure when the user places his finger on a fingerprint sensor, changes in pose and expression when the user stands in front of a camera, etc.), use of different sensors during enrollment and
verification, changes in the ambient environmental conditions (e.g., illumination changes in a face recognition system) and inherent changes in the biometric trait (e.g., appearance of wrinkles due to aging or presence of facial hair in face images, presence of scars in a fingerprint, etc.) (Ramachandra et al., 2012).

Ideally, the features extracted from the biometric data must be relatively invariant to these changes. However, in most practical biometric systems the features are not invariant and therefore complex matching algorithms are required to take these variations into account. Large intra-class variations usually increase the False Non-Match Rate (FNMR) of a biometric system.

**(e) Susceptibility to circumvention:** Although it is very difficult to steal someone’s biometric traits, it is still possible for an impostor to circumvent a biometric system using spoofed traits. Studies by Matsumoto et al. (2005) have shown that it is possible to construct gummy fingers using lifted fingerprint impressions and utilize them to circumvent a biometric system. Behavioral traits like signature and voice are more susceptible to such attacks than physiological traits. Other kinds of attacks like spoofing, replay and denial of service (DOS) can also be launched to circumvent a biometric system (Ratha et al., 2001). Due to these practical problems, the error rates associated with unimodal biometric systems are quite high which makes them unacceptable for deployment in security critical applications.

Ruggles (2002) stated that the use of biometrics has several drawbacks. The problems related to the human factor are major consideration. Unfortunately, the human bodies are constantly experiencing physical changes, such as injury, the worn out as the impact of the environment, etc. In addition, the different categories of users will have trouble with some biometrics. Physically disabled users may have trouble with the authentication systems based on fingerprints, hand geometry, or signature. There are also practical problems associated with biometrics. When biometrics is used for personal identification, biometrics technology measures and analyzes behavioral and physiological characteristics of the human being and identifies the physiological characteristics of a
person based on direct measurements of the parts of body - fingerprints, hand geometry, facial geometry and eye retinas and irises.

The effectiveness of utilization of biometric systems such as fingerprint, iris / retina scans and electronic signatures are measured by using quality indicator system. This is based on classifier combination where the sum and Max rules are used in combination so as to eliminate estimation errors.

2.2.2 Multimodal Biometric System
Multimodal biometric systems utilize more than one physiological or behavioral characteristic for enrollment, verification, or identification. It can provide reliable and secure applications than unimodal biometric system due to multiple pieces of evidence (Khan et al., 2006). Firstly, it can also provide reducing false non-match and false match rates. Secondly, it can provide a secondary means of enrollment, verification and identification if sufficient data cannot be acquired from a given biometric sample and thirdly, it can combat attempts to spoof biometric systems through non-live data sources such as fake fingers (Gandhimathi & Radhamani, 2014). Basing on these advantages this research will adopt a multimodal stance so as to ensure universality when using the biometric security system.

2.3 Biometric Security Technologies and their Effectiveness
The rising tide of data breaches and sophisticated hacking attacks of sensitive information, demands for a stronger and more secure way of protecting assets (Hussain, 2016). A biometric security system is a pattern recognition system that operates by acquiring biometric data from an individual, extracts a feature set from the acquired data, and compares this feature set against the template set in the database (Anil et al., 2004). The BST offer sophisticated security methods that are more effective in authentication and have profound advantages. The effectiveness of BST is inherent in the fact that the technology employed in the system can successfully give the result that the users expect when performing their tasks. Implementation of BST provides stronger reliability and security to increase security, convenience and realistic cost savings (Hussain, 2016).
A biometric represents the most secure and convenient authentication tool because it cannot be borrowed, stolen, or forgotten (Liu & Silverman, 2001). Generally, biometric systems adopt the model as shown in figure 2.11:

![Figure 2.11 Block Diagram of General Biometric System](image)

Biometric system as shown in Figure 2.11 typically operates in three phases which are enrollment, identification and verification. In the enrollment stage, a person provides an identifier (e.g. National identification number, Personal Identification Number, passport, Driving License) and his/her Biometric is linked to the identifier provided (Rogerberto, 2012). This Biometric is stored in the form of a template in the system database. Here the Quality Checker or the Sensor module captures the Biometric data of an individual from the user interface. From this information, the salient features that are uniquely used to identify an individual are grabbed by the Feature Extraction module. The System Database Module is then used to store the Biometric templates. During the Verification or Identification phases, a Matcher module is used to determine whether the user is valid.
In the Verification mode, a person provides his identity and a Biometric which is compared with his/her reference template. The user claims his identity through a User name, PIN, or Smart card and is verified to check whether the claim is true. The comparison here is one-to-one. A template is loaded from the System Database and then checked against the sample template. Two kinds of errors are possible during the verification phase. The False Reject Rate (FRR) or False Non Match Rate (FNMR) a condition in which a legitimate user is rejected by the user. The False Accept Rate (FAR) or a False Match Rate (FMR) is the likelihood of an impostor being accepted by the system as a genuine user (Anil et al, 2004).
In the mode, the system recognizes an individual by searching the templates of all the users in the database and compares them for a match (Kumar & Ryu, 2009). Therefore, the system conducts a one-to-many comparison to establish an individual’s identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (Anil et al, 2004).

![Figure 2.10 Block Diagram of the Verification phase adapted from Kumar & Ryu, 2009](image)

During the enrollment phase, a biometric feature set is extracted from user’s biometric data and a template is created and stored. During the verification phase, the same feature extraction algorithm is applied to query biometric data, and the resulting query feature set is used to construct a query template. The query template is matched against the stored template(s) for authentication in the identification phase (Sui et al, 2011). Compared to password/smartcard-based authentication approaches, biometrics-based solutions have many desired features such as being more resistant to losses incurred by theft of passwords and smartcards, as well as user-friendliness (Du et al, 2010). Biometrics bears a user’s identity and it is not easy to be forged. The basic aim of using biometrics is to devise a mechanism that is more secure in protecting the cryptographic key of a user as compared to the conventional method of password-based encryption (Ahmed & Siyal, 2005). Thus biometrics offers an increasingly attractive solution like a ‘key’ that the user cannot lose or forget (Gifford et al., 1999).
Today there are lots of biometric technologies available. A few of them are in the stage of research only (e.g. the odor analysis), but a significant number of technologies is already commercially available and has been implemented for use. These technologies include signature dynamics, fingerprint recognition, iris recognition, facial-scan technology, hand geometry, retinal scan, vascular patterns and voice dynamics. They are discussed hereunder:

2.3.1 Signature Dynamics

Signature recognition is based on the dynamics of making the signature acceleration rates, directions, pressure, and stroke length rather than a direct comparison of the signature after it has been written. This recognition is the task of recognizing an individual by using their signatures. Signature is a behavioral biometric, the features of signature are variant with respect to time. The problems with signature recognition are in the means of obtaining the measurements used in the recognition process and the repeatability of the signature.

The instrumentation cannot consistently measure the dynamics of the signature. Also a person does not make a signature in a fixed manner therefore; the data obtained from any one signature from an individual has to allow for a range of possibilities. Furthermore, forgers can easily fool the system by reproducing the signatures of the correct persons. Irrespective of the above limitation we can still use signature as our best biometric feature, since the signature is a unique identity of an individual and is being used extensively in practical systems. No two signatures can be identical, unless one of them is a forgery or copy of the other (Ammar et al., 1990). Signature verification is the verification of given signature of claimed identity of a person.

There are two types of signature verification systems in practice, namely, online and offline (Nalwa, 1997). Online signature verification uses information collected dynamically at the time of signature acquisition like timing, acceleration, velocity, pressure intensity and also termed as dynamic signature verification. Offline signature verification uses only the scanned image of signature and also termed as static signature verification. In case of online signature verification during the training phase, the user supplies a set of reference signatures measured in terms of dynamic features mentioned
above. These dynamic features along with signatures are stored as reference templates. When a test signature is input to the system in terms of these dynamic features, it is compared to each of the reference signatures of the claimed person. Based on the resulting comparison distance, the claimed identity is either accepted or rejected. Most of the existing signature verification systems are based on online approach.

2.3.2 Fingerprint Recognition

Fingerprint recognition is perhaps the oldest of the biometric sciences. This recognition is the most consistent biometric modality in use, since digital fingerprints are more convenient and less disturbing than most of the other biometric methods and they are already accepted as an immutably single identifier (Maltoni et al., 2003). A fingerprint is the feature pattern of one finger. It is composed of ridges and furrows that present good similarities in each small local window, like parallelism and average width. Fingerprint comparisons today are based on ‘Minutiae’ individual unique characteristics within the fingerprint pattern.

The fingerprint recognition field can be grouped into two sub-domains: the verification step and the identification step. The verification step consists in confirming the authenticity of one person by his fingerprint. The user provides his fingerprint together with his identity information and the system retrieves the fingerprint template according to the ID number and matches the template with the real-time acquired fingerprint from the user (Magnus, 2001). Fingerprint identification is to specify one person's identity by his fingerprint(s). Without knowledge of the person's identity, the fingerprint identification system attempts to match his fingerprint(s) with those in the fingerprint database. Fingerprint images contain a large amount of data. Because of the high level of data present in the image, it is possible to eliminate false matches and quickly reduce the number of possible matches to a smaller number, even with large database sizes. This is due to the fact that fingerprint imaging systems use more than one finger image in the match process as such the match discrimination process is geometrically increased.

It is particularly useful for criminal investigation cases. However, all fingerprint recognition problems, either verification or identification, are ultimately based on a well-defined representation of a fingerprint (Davies & Chang, 1994). However today,
fingerprint identification has undergone an extensive research and development and because of this fingerprint identification process has a 98% + identification rate and false positive identification rate is less than 1%.

2.3.3 Iris Recognition

The iris is the colored part of the eye behind the eyelids, and in front of the lens. The function of the iris is to control the amount of light entering through the pupil by the sphincter and the dilator muscles, which adjust the size of the pupil (Jhon, 2003). Iris recognition is based on the characteristics in the iris of the eye. These visible patterns are unique to all persons and the chance to find two individuals with identical iris patterns is about zero. However the person has to stand approximately 12-14 inches from the camera which frame- grabs an image of the iris for analysis.

For a developed approach of iris recognition, the input is an eye image, and the output is the iris template - a mathematical representation of the iris region (Libor, 2003). The algorithm consists in 3 steps: segmentation, normalization and feature encoding. Segmentation: Consists of separating the iris region in two circles: the iris/sclera boundary and the iris/pupil one. This step is decisive to the success of an iris recognition system, since wrong iris pattern will alter the generated biometric templates, and cause poor recognition rates (Xiaomei, 2006). This is followed by normalization; at this level once the iris region is successfully segmented, it’s transformed into fixed dimensions in order to tolerate upcoming comparisons. The dimensional variations between different eye images are generally due to the iris stretching caused by pupil dilation from varying levels of illumination.

The last step is Feature Encoding: this step entails the extraction of the most discriminating information of the iris pattern and encoding their significant features to facilitate templates comparisons. The generated template requires a related matching metric to measure similarity between iris templates generated from the same eye (intra-class comparisons), and templates created from different irises (inter-class comparisons). These measures should be distinguishable to highlight confidence in judging whether two templates are from the same iris or from two different irises.
An iris scan produces a high data volume which equates to a high discrimination rate (identification rate). Iris scan technology may be more acceptable to the user than retinal scans because as opposed to retinal scans, it does not use infrared light source to highlight the biometric pattern in the iris. However it has not fully developed and is currently under prototype testing making its implementation a challenge.

2.3.4 Facial-Scan Technology

Another biometric scan technology is facial recognition. This technology is considered a natural means of biometric identification since the ability to distinguish among individual appearances is possessed by humans. For investigation purposes, facial recognition was categorized into different parts of the face like the chin, hair line, nose features and mouth features. These were grouped into sets of templates that could be assembled into a composite face which would hopefully; resemble the face of the person in question.

Today facial scan systems can range from software-only solutions that process images processed through existing closed-circuit television cameras to full-fledged acquisition and processing systems, including cameras, workstations, and backend processors (Manoj, 2003). Facial recognition technology has developed into two areas; Facial Metrics: relies on the measurement of specific facial features for example, the distance between the inside corners of the eyes, the distance between the outside corners of the eyes and the outside corners of the mouth and the relationship between these measurements.

Eigen faces: categorizes faces according to the degree of fit with a set of other Eigen faces. It has been postulated that every face can be assigned a degree of fit to each of 150 Eigen faces. Eigen face information is derived from a computer – based analysis of the digital image of the photo. Eigen faces are (reportedly) highly repeatable and are not affected by human subjectivity. Although quite promising the Eigen face technology is in its infancy stage of development and very little data regarding Eigen face error rates (false negative, false positive) exists.
With facial recognition technology, a digital video camera image is used to analyze facial characteristics such as the distance between eyes, mouth or nose. These measurements are stored in a database and used to compare with a subject standing before a camera. Facial recognition systems are usually divided into two primary groups. First there is what is referred to as the ‘controlled scene’ group whereby the subject being tested is located in a known environment with a minimal amount of scene variation. In this case, a user might face the camera, standing about two feet from it (Samir, 2002). The system locates the user's face and performs matches against the claimed identity or the facial database. It is possible that the user may need to move and reattempt the verification based on his facial position. The system usually comes to a decision in less than 5 seconds.

The other group is known as the “random scene” group where the subject to be tested might appear anywhere within the camera scene (Zeena, 2002). This situation might be encountered within a system attempting to identify the presence of an individual within a group or crowd. This situation was evidenced since 11 Sept when security personnel stated that facial scan recognition technology would be used at a Super bowl game. Facial-scan technology is based on the standard biometric sequence of image acquisition, image processing, distinctive characteristic location, template creation, and matching (Julian, 2002). An optimal image is captured through a high-resolution camera, with moderate lighting and users directly facing a camera. The enrollment images define the facial characteristics to be used in all future verifications, thus a high-quality enrollment is essential. Challenges that occur in the image acquisition process include distance from user, angled acquisition and lighting. Distance from the camera reduces facial size and thus image resolution. This could in turn distort the image formed on the template and in turn return a false match rate.

2.3.5 Hand Geometry
All biometric techniques differ according to security level, user acceptance, cost, performance, etc. One of the physiological characteristics for recognition is hand geometry, which is based on the fact that each human hand is unique and is shaped differently than another person’s hand (Varchol & Levicky, 2007). It also affirms that
after a certain age a person’s hand does not significantly change in its shape. Features like, finger length, width, thickness, curvatures and the relative location of these features distinguish every human being from any other person (Varchol & Levicky, 2006).

The availability of low cost, high speed processors and solid state electronics made it possible to produce hand scanners at a cost that has made them affordable in the commercial access control market. There are two methods to measure the hand; mechanical and image edge detection. Either method produces estimates of certain key measurements of the hand (length of fingers and thumb, width). This data is then used to categorise a person.

However environmental factors such as dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy of hand geometry-based systems (Kung et al., 2004). The performance of these systems might be influenced if people wear big rings, have swollen fingers or no fingers. Although hand analysis is most acceptable, it was found that in some countries people do not like to place their palm where other people do. Sophisticated bone structure models of the authorized users may deceive the hand systems. Paralyzed people or people with Parkinson's disease will not be able to use this biometric method.

Also, hand geometry, does not produce a large data set. Therefore given a large number of records, hand geometry may not be able to distinguish one individual from another who has similar hand characteristics. This is because with hand geometry there is not enough data available; the individual is placed in a ‘band’ within the database structure that contains many individuals. Because of the complexity of hand geometry use it’s prohibitively quite expensive.

2.3.6 Retinal Scan
It’s based on the blood vessel pattern in the retina of the eye. An infra-red light is used to illuminate the retina of the eye; the infra-red energy is absorbed faster by blood vessels in the retina than by the surrounding tissue. The image of the enhanced blood vessel pattern of the retina is analysed for characteristic points within the pattern. A retinal scan can produce almost the same volume of data as a fingerprint image analysis. Based on the
fact that a high data volume equates to a high discrimination rate (identification rate), it would seem that retinal scan may be an alternative to fingerprint identification.

However retinal scan technology has several drawbacks that are not common to fingerprint imaging technology; the retinal scan is more susceptible to disease (notably cataracts) that change the characteristics of the eye, the method of obtaining a retina scan is personally invasive that is a laser light (or other coherent light source) must be directed through the cornea of the eye, the method of obtaining a correct retinal scan depends heavily on the skill of the operator and the ability of the person being scanned to follow directions.

Retinal scan technology has not had the level of research and development funding (both from private and government sources) that fingerprint imaging technology has had within the past twenty years.

2.3.7 Vascular Patterns

Vascular pattern technology is very similar to retinal scan technology I that it uses infra-red light to produce an image of the vein pattern in the face, in the back of the hand or on the wrist. Vascular pattern technology is generally acceptable to users except that some users still object to any biometric method that uses infra-red.

2.3.8 Voice Dynamics

This relies on the production of a “voice template” that is subsequently used to compare with a spoken phrase. A speaker must repeat a set phrase several times as the system builds the template. This biometric technology relies on the behaviour of the subject rather than the physical characteristics of the voice and is therefore prone to inaccuracy.

These are just but a few technologies that have been employed in the creation of biometric systems. Many more exist (for example DNA and ear geometry) but have not been mentioned here because this study aims to incorporate only those technologies that
will be established after analyzing the collected data to create a security system that can cater for all users.

Wilkinson (1992) proposed eleven indicators that could provide measurements to assess whether the existing systems are effective and efficient. The eleven indicators are: relevant (as needed), capacity (of the system), efficiency (of the system), timeliness (in yield), accessibility (ease of access), flexibility (flexibility of the system/device), accurate (the accuracy of the value of the information generated by the device / system), reliability (the reliability of the system/device), security (of the system/device), economic (economic value of the system/device) and simplicity (ease of system/device).

One other factor that influences the effectiveness of a BSS is its level of adoption. Adoption of new technologies has proved difficult the world over. This is because there is fear amongst the users that the new technology might not be effective or as efficient like the old systems. In addition, there are factors that influence how the new technology is received and used. Given that human beings are as diverse as their numbers, Grunwald (2002) identifies various characteristics that influence an individual’s adoption to a security system. These characteristics are potential adopter traits: risk aversion, gender; potential adopter usage style; personal conviction, motivation, experience, self-efficacy, academic discipline and age.

Individual difference characteristics include things like personality and/or demographics (e.g., traits or states of individuals, gender, and age) that can influence an individual’s perceptions of perceived usefulness and perceived ease of use of technology (Venkatesh & Bala, 2013). It’s presumed that such factors create techno-phobia, a condition in which an individual will not fully participate or venture into the use of new technology until it’s demystified to them (Lewicka, 2011).

Other factors that influence the effectiveness of BST are forces within the society for example family, friends, colleagues, neighbors and the media. Such social forces influence how an individual selects or uses technology (Bala, 2008). This is because they contribute to our social lives and have direct effect to factors like our Lifestyles, attitudes and beliefs, opinions and interests, social mobility, education, demographics, ethics and
religion, historical issues and cross cultural communications and in the long run affect the choice of technology/security system by an individual.

There are also other factors that are organizational related and have a significant impact on the acquisition and implementation of BST. Such factors include top management support, organization size, technological readiness of the organization, extent of functional integration and physical dispersion/number of collaborating organizations (Rains & Young, 2006). These factors influence the way employees in an organization adopt and effectively use a BST but more often than not the changes that impact effectiveness of BST in an organization come from unexpected sources (Ndekwa, 2014). These are key factors for organizations as they help in assessing how effective an adopted BST is as well as list the issues that could have a potential impact on the organizations operations and that could be critical to its long-term future efficiency of the BST (Iyer & Handerson, 2012).

On the other hand, technological factors are mainly influences that have an impact on how an organization operates that is related to the equipment used within the organizations environment? These include, rate of change, use of outsourcing, research and development, knowledge management systems, network coverage, production efficiency, quality pricing, intellectual property, patents and licenses and government activity and legislation (Brainin & Ezrez, 2004). It’s important to note that an organization's ability to change and adopt the use of BST is influenced by many factors, including its competence, sophistication, and history of action with other technologies.

2.4 Recognition Performance of Unimodal Biometric Security Systems

BST is very complex both in its ability and its performance, thus biometric system typically uses additional tools such as cameras and scanning devices to capture images, to record, or to measure the characteristics of a person, and a computer software / computer hardware to extract, to encode, to store, and to compare those characteristics. In the design of Biometric systems, the designer undertakes the development in a four stage process comprising of capture, extraction, comparison and appropriate/not appropriate. In the capture stage, the designer develops software and hardware for a biometric system to collect samples of biometric features such as fingerprints or voice of the users who would log into the system.
In the extraction stage, the system is developed in such a way to extract data that is used to uniquely create samples and templates. Unique features are then extracted by the system and converted into digital code biometrics. The sample is then stored as the biometric template for that individual in the systems database.

At the comparison stage, the template is then compared with the new sample. Biometric data is then stored as the biometric template or template reference to that person. Lastly is the appropriate / not appropriate stage that involves the system to decide whether the features extracted from the new sample are appropriate or not with the template. If the features extracted are appropriate with the template in the BST database the user is allowed to access the resource in question, but, if the result is inappropriate then the user is denied service basing on the rejection rate of the system.

However, BST performance also depends on other factors such as usability and/or user acceptance which can significantly affect the system performance. These factors include a variety of ways to present the biometric characteristics for sensors and the variability of biometric characteristics caused by disease or climate changes.

Table 2.1 provides various rates emanating from several test rates used in determining recognition performance of unimodal BSS. From the table, tests carried out on fingerprint biometric technology using fingerprint verification competition (FVC) revealed that there is no remarkable difference in the rates of false rejection rate (FRR) or false acceptance rate (FAR) if the parameter under study is exaggerated skin distortion or rotation. However, if the fingerprint vendor technology evaluation test (FpVTE) is employed and the test parameter is operational data from the government then FAR is higher than FRR. Furthermore, when using face biometric technology, if both indoor and outdoor lighting is varied and the face recognition verification test (FRVT) is employed the results reveal higher FRR compared to FAR. Lastly according to NIST report tests performed on voice biometrics reveal high FRR for tests in text independent multilingual compared to FAR.

**Table 2.1: State-of-the-art error rates associated with fingerprint face and voice biometric systems.**
<table>
<thead>
<tr>
<th>Biometric</th>
<th>Test</th>
<th>Test Parameter</th>
<th>False Reject Rate (FRR)</th>
<th>False Accept Rate (FAR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint</td>
<td>FVC 2004</td>
<td>Exaggerated skin distortion, rotation</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td></td>
<td>FpVTE 2003</td>
<td>US government operational Data</td>
<td>0.1%</td>
<td>1%</td>
</tr>
<tr>
<td>Face</td>
<td>FRVT 2002</td>
<td>Varied lighting, outdoor, indoor</td>
<td>10%</td>
<td>1%</td>
</tr>
<tr>
<td>Voice</td>
<td>NIST 2004</td>
<td>Text independent multilingual</td>
<td>5-10%</td>
<td>2-5%</td>
</tr>
</tbody>
</table>

These limitations in the performance of unimodal biometric system are positively overcome with use of multiple source of information from the user, which also increases the security of the system (Matsumoto et al., 2005). A multimodal biometric system is one that can consolidate cues obtained from two or more biometric sources for the purpose of person recognition.

2.5 Security Levels Assessment in Systems

Simply put, an information security assessment is a measurement of the security posture of a system or organization (Miles et al., 2004). The security posture is the way information security is implemented. Security assessments are risk-based assessments, due to their focus on vulnerabilities and impact. Security assessments rely on three main assessment methods which are inter-related. These methods are review method, examination method and testing method. When the three methods are combined, they can accurately assess technology, people, and process elements of security (SANS, 2008).

2.6.1 Reviewing Method

The reviewing method includes passive review techniques and interviews, which are generally conducted manually. They help to evaluate systems, applications, networks, policies, and procedures to discover vulnerabilities. They include the review of
documentation, architecture, rule-sets, and system configurations. The reviewing method enables understanding what the critical information & systems are, and how the organization wants to focus on security.

2.6.2 Examination Method
Examination is a hands-on technical process that looks specifically at the organization from a system/network level to identify security vulnerabilities that exist in those systems. This includes doing technical analysis of the firewalls, intrusion detection systems, and routers. It also includes vulnerability scans of the customer’s networks. The reviewing assessment method provides excellent information that leads into future examinations.

2.6.3 Testing Method
Testing, often called penetration testing, is a process whereby someone imitates an adversary looking for security vulnerabilities, which allow the break in to a system or network. Reviewing and examination methods provide excellent information that leads into future testing. The diagram below illustrates the methods’ relationship (Miles et al., 2004).

A security assessment is performed to identify the current security posture of an information system or organization. The assessment provides recommendations for improvement, which allows the organization to reach a security goal that mitigates risk, and also enables the organization, take the necessary measures. Since no one technique can provide a complete picture of the security of an information system or network, organizations should combine appropriate techniques to ensure robust security assessments.

2.6 Technology Adoption Theories
The decision of whether an individual will adopt a particular technology (like BST use) and the time frame involved with that decision has been a long source of research across multiple disciplines (Davis et al., 1989). Its therefore essential to understand various aspects of the adoption process such as the following; why does one individual choose to adopt a technology while another resists? What is the influence of social context on the decision to adopt? These questions are addressed in the context of adoption, acceptance and diffusion theories or models. Since an innovation like the BST is a new idea to a population (Rogers, 1995) an adoption theory will examine the individual and the choices
he/she makes to accept or reject a particular innovation, while in a model adoption is not only the choice to accept an innovation but also the extent to which the innovation is integrated into the appropriate context.

There are various theories and models used in the research of adoption of new technologies; to investigate the determinants of acceptance and use of new biometric technology this study adopts four models. The models discussed here include Technology Acceptance Model (TAM) (Adams et al., 1992; Davis, 1986; Davis et al., 1989) and Technology Organization Environment Framework (TOEF). Another model that is frequently used in information technology to explain user adoption of new technologies that will be adopted here is Rogers’ (1983) Diffusion of Innovation (DOI) theory and Unified Theory of Acceptance and Use of Technology (UTAUT). The determinants for the adoption of technology based on these models comes from the individual beliefs, attitudes, subjective norm, perceptions of behavioral control, perceived usefulness and its perceived ease of use.

2.4.1 Technology Acceptance Model

Based on the theory of reasoned Action, (Davis, 1986) developed the Technology Acceptance Model which deals more specifically with the prediction of the acceptability of an information system. The purpose of this model is to predict the acceptability of a tool and to identify the modifications which must be brought to the system in order to make it acceptable to users. This model suggests that the acceptability of an information system like the BSS is determined by two main factors: perceived usefulness and perceived ease of use.

Perceived usefulness is defined as being the degree to which a person believes that the use of a system will improve his performance. Perceived ease of use refers to the degree to which a person believes that the use of a system will be effortless. Several factorial analyses demonstrated that perceived usefulness and perceived ease of use can be considered as two different dimensions (Hauser & Shugan, 1980; Larcker & Lessig, 1980; Swanson, 1987). The Technology Acceptance Model postulates that the use of an information system like BSS is determined by the behavioral intention, but on the other
hand, that the behavioral intention is determined by the person’s attitude towards the use of the system and also by his perception of its utility.

According to Davis, the attitude of an individual is not the only factor that determines his use of a system, but is also based on the impact which it may have on his performance. Therefore, even if an employee does not welcome an information system, the probability that he will use it is high if he perceives that the system will improve his performance at work. Besides, the Technology Acceptance Model hypothesizes a direct link between perceived usefulness and perceived ease of use. With two systems offering the same features, a user will find more useful the one that he finds easier to use (Dillon & Morris, 1996). This is well elaborated in figure 2.1 below.

![Technology Acceptance Model](image)

Figure 2.1: Technology Acceptance Model (Davis et al, 1989)

Nevertheless TAM has limitations, some researchers argue that constructs in TAM are not sufficiently enough to predict the users’ intention and there is lack of other constructs that can be used for better understanding (Kulviwat et al., 2007). They argue that other predictive variables such as Subjective Norm, Social Influence, Perceived Enjoyment and Critical Mass must be taken into close consideration in individual IT acceptance.

2.4.2 Innovation Diffusion Theory (IDT)

IDT has been used since the 1950s to describe the innovation-decision process and it’s acknowledged to have evolved just a few times (Rogers, 1962; Rogers, 1983; Rogers, 1995; Rogers & Shoemaker, 1971). According to the innovation-decision process, an individual or decision making unit, passes from first the knowledge of an innovation, then to forming an attitude toward the innovation to a decision to adopt or reject to
implementation of the new idea and to confirmation of this decision.

The entire model is more focused on the process of diffusion rather than adoption, see figure 2.2. Aspects of adoption that are explored by this study are merely addressed, as a decision, either for rejection, immediate adoption, later or continuous adoption or for continued rejection. The model, though not very comprehensive for studying adoption, has a valuable basis for this study, particularly the persuasion characteristics and prior conditions that an organization can put in place to enable the employees adopt and use a new technology.

Figure 2.2: Innovation Diffusion Model (Rogers, 1995)

However this theory has some limitations; it does not consider the possibility that people will reject the innovation even if they fully understand it (Waterman, 2004; Botha & Artkins, 2005).

Also it’s important to note that insufficient consideration is given to innovation characteristics and how these change over time (Wolfe, 1994). This theory is not well supported because it tends to emphasize the fact that all members of a social system should adopt innovation and adoption should happen quickly. According to Kole, 2000, this theory does not take into account the fact that diffusion and adoption may fail
because maybe it was a bad idea to begin with or that the theory associates the latest technologies with progress thereby ignoring alternatives and that these theory focuses on the individual adopter and therefore ignoring the social structures.

Other authors like Nutley et al., (2002) argue that the nature of utilization of knowledge in this theory can be very complicated by contrasting straight forward adoption (replication) versus reinvention (adaptation). Early studies of the diffusion theory assumed that innovation meant copying or imitating how the innovation had previously been used even if the situation was different. Charters and Pallegrin (1992), proposed that the concept of re-invention should be adopted which means the degree to which an innovation is changed or modified by the user in the process of its adoption and implementation.

2.4.3 Technology, Organization and Environment Framework (TOE)

The TOE framework, as shown in figure 2.3 was developed in 1990 (Tornatzky & Fleischer, 1990). It identifies three aspects namely, technological innovation context, organizational context, and environmental context. These aspects influence the process by which an organization adopts and implements a technological innovation.
Figure 2.6: Technology, organization, and environment framework Adapted from, Tornatzky and Fleischer, 1990

The TOE provides a useful analytical framework that can be used for studying the adoption and assimilation of different types of IT innovations in various organizations. It has a solid theoretical basis, consistent empirical support, and the potential of application to IS innovation domains like BSS, though specific factors identified within the three contexts may vary across different organizations.

2.4.4 Unified Theory of Acceptance and Use of Technology (UTAUT)

UTAUT provides a refined view of how the determinants of intention and behaviour evolve over time (Venkatesh et al., 2003). In addition, it is important to emphasize that most of the key relationships in the model are moderated. The UTAUT model has been praised for its capability to inform the understanding of factors, which determine the acceptance of an impending new technology. Although the model is quite new, its growth and popularity is increasingly high as compared to the preceding versions (Dwivedi, 2012). Moreover, its stability, validity, and viability in technology adoption surveys within several contexts have already been ascertained and practically confirmed. UTAUT model enlightens the understanding of factors, which influence the acceptance of a vital new technology (Chhabra, 2013).

The UTAUT, as shown in Figure 2.4 was introduced with four core determinants of intention and usage, and up to four moderators of key relationships. The UTAUT formulated four constructs to play an important role as direct determinants of user acceptance and usage behaviour: these are Performance expectancy, Effort expectancy, Social influence and Facilitating conditions.
Most importantly, UTAUT model explains over 70% of all the technology acceptance behaviour, unlike other forms of models that explain as little as 40% of the entire technology acceptance behaviour. Therefore, UTAUT exposes more factors influencing the intention of the observed behaviour (ICIME, 2011). Ultimately, it was intended to counter the deficiencies of prior models and theories by combining them together for a common good. For that reason, it has emerged as one of the most encompassing IT adoption theories (Woodside & Kozak, 2014).

Even though this model has attained an adequate reception from most researchers, a number of shortcomings exist. Although each of the models utilizes several terminologies within their phraseology of acceptance, these aspects are often similar in nature. Subsequently, every model has its own shortcomings, which also influences the ultimate viability of UTAUT model as a whole (Gasco, 2012). UTAUT has limitations mainly in its relationship between the intention and use of behaviour. Nevertheless, the benefits obtained from this model are far more significant than the shortcomings listed above (International Conference on E-Learning, 2014).
Based on its limitations, researchers resolved to add precipitating occasions in order to measure the impact of external factors like government policy, and new markets on Information Technology innovations. They observed the impact of the tendency to act as a diplomat among the determinants intentions and usage behaviour. It was noted that where tendency to act is high, taking action might be more probable (United Nations, 2012). Based on UTAUT limitations, researchers added precipitating events so as to measure the impact of external aspects like government policy, new markets, and financial crises. They added these factors to IT innovations and adoption and scrutinized the impact of propensity to perform as a moderator on the association between the determinants intention and custom behaviour.

It was noted that where the condition of propensity is high, taking action will be more foreseeable. Based on research, it is evident that precipitating occasions might capture the influence of external aspects on the behavioural intention to make a start, enhance the model, and fill intention-behaviour gap (Wanamina et al., 2014). In that case, it is evident that entrepreneurs have different perception on UTAUT because some of them believe that it is a fairly developed model. As a result, this has influenced more than a few organizations to consider other types of models apart from UTAUT (Xiang & Tussyadiah, 2013).

These models are important to any organization as they help the organization understand how to easily diffuse new technologies into the work processes of the organization.

2.7 The Assessment Tool
Information system model assessment activities are certainly not new within the field of system development (Mumford et al, 1978). But it is only recently that the literature on system development has generally recommended formal procedures for information system model assessment (Nordbotten, 1985). In the prevalent tradition, different techniques were proposed for gathering and processing information concerning the performance of the new model and the organization. The purpose of these proposed techniques was to determine whether the new or changed system has met its objectives (Preben & Kim, 1988). The collected and processed information is therefore considered an important basis for the subsequent maintenance or adjustment of the model.
The acknowledgement of assessment as an important part of the life cycle of an information system model is, on one hand, a valuable progress. But, on the other hand, it is regrettable that assessment has been based on the same assumptions over the years. The general wisdom has been dominated by a very narrow understanding of success or failure of the information system models. According to Senn (1985), analysts of a system model want to know if the performance level of users has improved and if the information system model is producing the intended results.

In assessment, a tool is designed for documenting and making representations of the situation. Descriptions are made with the purpose of communicating the result of the assessment. The basic concept is a fixed set of values or categories, that is, depending on the system model characteristics being evaluated, a number of separate measures may be used. Various assessment tools have been designed and implemented. Preben & Kim (1988) designed a Library Information System (LIS) assessment tool where unstructured descriptions were used as a tool for clarifying and interpreting the situation at the library on the library information system.

Munshi et al (2009) prescribed health metrics network (HMN) assessment tool that was used to assess the country status of Health Information System (HIS). This was a comprehensive tool provided by the HMN secretariat in Geneva to assess the country’s Health Information System on the basis of several specific components. Scoring was done on each item of the HMN assessment tool of the HMN framework. The HMN framework has six components as given below:

- HIS resources
- Indicators
- Data sources
- Data management
- Information products
- Dissemination and use

These were further categorized into inputs, processes, outputs and impacts. For this study, the assessment tool will be designed to validate the model that will be prototyped after data analysis basing on the eleven characteristics proposed by Wilkinson in 1992. These
characteristics will be tailored into a template that the users will use to validate the model to check whether it meets the set objectives of the study.

Statistical tools in modeling include Bayesian Structural Equation Modeling, Gaussian Equation, Euclidean Equation and the combination approach including the Sum Rule, Product Rule, Min Rule and Max Rule. This study will use a combination approach to modeling which will utilize the strengths various models to analyse the resulting data. These models have been discussed hereunder:

2.7.1 Bayesian Structural Equation Modeling

In recent times, the Bayesian tools have gained increased use due to advancements in computational algorithms based on Markov Chain Monte Carlo (MCMC) sampling (Kaplan & Depaoli, 2012). Kaplan and Depaoli (2012) explain that in Bayesian inference, a vector \( Y \) could hold a very large set of data such as; \( y_1, y_2, \ldots, \), where \( Y \) is unobservable characteristic and \( y_1, y_2 \) are the actual observed (realized) values. The tool sets to determine the probability of observing \( y \) given unknown parameter \( \theta \), written as \( p(y|\theta) \). On the other hand, statistical inference aims at finding the likelihood of parameters given the data, this is denoted as \( L(\theta|y) \) which can also be obtained in logarithmic notation as \( l(\theta|y) \). If the observed data \( y \) and the parameters \( \theta \) are assumed random then the model of the joint probability of the parameters and the data is a function of the conditional distribution of the data given the parameters and the prior distribution of the parameters (Kaplan & Depaoli, 2012). That is:

\[
p(\theta|y) = p(y|\theta)p(\theta)
\]

Where \( p(\theta|y) \) is referred to as the posterior distribution of the parameters \( \theta \) given the observed data \( y \).

\[
p(y|\theta)p(\theta) = p(\theta|y)p(y)
\]

Therefore, the posterior distribution of \( (\theta) \) given \( y \) is equal to the data \( p(y|\theta) \) times the prior distribution of the parameters \( p(\theta) \) normalized by \( p(y) \) so that the distribution integrates to one. This is shown in equation below:

\[
p(\theta|y) = \frac{p(\theta, y)}{p(y)} = \frac{p(y|\theta)p(\theta)}{p(y)}
\]
Below is the Bayesian theorem for discrete variables:

\[ p(y) = \sum_\theta p(y|\theta)p(\theta) \]

### 2.7.2 Gaussian Modeling

### 2.7.3 Combination Approach

In this approach, the matching scores are converted in posterior probabilities that conform to a genuine user or an impostor. According to Jain, Nandakumar and Ross (2005), an input pattern \( Z \) is classified into one of \( m \) possible classes where in a verification system \( m = 2 \), based on the evidence provided by \( R \) different classifiers. They stated that if \( \vec{x}_i \) is the feature vector (derived from the input pattern \( Z \)) presented to the \( i \)th classifier. If the outputs of the individual classifiers are \( P(\omega_j | \vec{x}_i) \) then the posterior probability of the pattern \( Z \) belonging to class \( \omega_j \) given the feature vector \( \vec{x}_i \).

If \( c \in \{1,2,3,\ldots, m\} \) is the class to which the input pattern \( Z \) is finally assigned, then the following the Product Rule, Sum Rule, Max Rule and Min Rule can be used to determine \( c \) as discussed below:

In Product Rule, various biometric traits of an individual are mutually independent. It is based on the assumption of statistical independence of the representations \( \vec{x}_1, \vec{x}_2, \ldots, \vec{x}_R \).

The input pattern is assigned the class \( c \) such that:

\[ c = \arg \max_j \prod_{l=1}^{R} P(\omega_j | \vec{x}_l) \]

For the Sum Rule, the assumptions are: statistical independence of the multiple representations and that the posterior probabilities computed by the individual classifiers do not deviate much from the prior probabilities. With high noise levels the Sum Rule is
better placed to rectify classification problems. In the Sum Rule, the input pattern is assigned to class $c$ as:

$$c = \alpha \sum_{j=1}^{R} P(w_j | \vec{x}_i)$$

In the Max Rule, the mean of the posterior probabilities are estimated by taking the maximum value of the scores. The input pattern $Z$ is assigned to class $c$ as:

$$c = \alpha \max_{j} m P(w_j | \vec{x}_i)$$

For the Min Rule, the score having the least value of the modalities is chosen (Fouda, 2012). According to Karanwal, Kumar and Maurya (2010), this rule is derived by bounding the product of posterior probabilities. The input pattern is assigned to class $s$ as:

$$c = \alpha \min_{j} m P(w_j | \vec{x}_i)$$

### 2.8 Research Gap

Insecurity levels are on the rise all over the world; hence most governments including Kenya have come up with stringent measures to guard their resources as well as their citizens. Organizations in Kenya today have employed some form of security measure but in most cases these are traditional systems whose security levels are weak. Biometric security systems are slowly creeping into the information systems world and taking over the traditional systems. Because they employ the use of physiological or behavioural characteristics for authentication it’s evident that they should be implemented, however that’s not the case. Although there are organizations in Kenya that have adopted the use of biometric systems, this adoption is done shyly and most of these systems are mainly unimodal. But such systems suffer from lack of accuracy, limitation in enrollment rates, and susceptibility to spoofing. Many authors have come up with models for adoption of biometric systems but in most cases these just incorporate two or three biometry. Even
so, these systems have not been adopted for use in most organizations despite it being a better technology for security of resources. This research therefore will attempt to design a model for adoption of multimodal biometric security systems using the fusion of various characteristics for universality purposes.

2.9 Theoretical Framework
Kittler 1998, in his study, focused on classifier combination and developed a common theoretical framework for classifier combination to show that many existing schemes can be considered as special cases of compound classification where all the representations are used jointly to make a decision. Kettler’s study demonstrated that using different approximations commonly used classifier combination schemes such as the product rule, sum rule, minimum rule, maximum rule, median rule, and majority voting can be derived. The various classifier combination schemes were then compared experimentally. The outcome was that the combination rule developed—the sum rule—outperformed other classifier combinations schemes. This study seeks to adopt the sum rule in the measurement of recognition performance level of unimodal biometric security systems in private organizations. The sum rule will be used in combination with the Min - Max rule for this study as it is more resilient to estimation errors.

2.10 Conceptual Framework
There are numerous forms of biometrics now being built into technology platforms. However biometric technology is relatively new and as such has not fully matured. This immaturity is not only limited to the technology itself, but extends to other areas such as legislation, standards and governance resulting in challenges relating on interoperability. The major contributor of technology advancement is the ever evolving user requirements, expertise training and competition among the manufacturers to meet these user needs. This study therefore, will be guided by the conceptual framework in Figure 2.9 where the independent variables will include the Biometric security systems available, the types of biometric technologies in use as well as the organizational factors influencing biometric security system adoption and how these affect the adoption of multimodal biometric security systems in organizations which is the dependent variable. The arrows indicate interrelationships between the key variables. The relationship
between the independent variables and the dependent variables will be affected by things like the available policies and standards, knowledge levels of the user, acceptability as well as usability.

**Independent Variables**

- Types of Biometric Security Systems
- Effectiveness of Biometric Security Technologies
- Recognition performance of unimodal biometric security systems

**Dependent Variable**

- Adoption of Multimodal Biometric Security System in Organizations

**Moderating Variables**

- Policies & Standards
- Knowledge levels of the User
- Acceptability
- Usability

*Figure 2.12: Conceptual Framework*
CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction to Research Methodology

This chapter outlines the following areas: the research philosophical approach, the research design, the research site, the target population, sampling as well as identifying the sample from the population, the research instruments, and quality control of the research instruments, data analysis and the ethical considerations to be adhered to.

3.2 Research Philosophy

Every research work is based on some underlying paradigm that directly informs what will constitute that research and the methods to be employed (Gill & Johnson, 2002). There are various paradigms that can be adopted in any research work. Although there will be areas in this study where interpretivism will be employed, this research will be grounded in pragmatism paradigm. Pragmatic approach to research involves using the method which appears best suited to the study (Baghramian, 2008).

Each observation made in this study will be quantified based on a measurement scale that will facilitate empirical analysis. The researcher’s role will be limited to data collection (Dudovskiy, 2016) that will enable an objective understanding of the research area. The adoption of this paradigm is informed by the fact that pragmatism approach grants freedom to the researcher to use any of the methods, techniques and procedures typically associated with quantitative or qualitative research (Brandon, 2004). Being able to mix different approaches in this study will be of advantage in that it will enable triangulation of a variety of data sources. The findings will then be used objectively to develop the model and the tool to assess it.

3.3 Research Design

A research design is the conceptual structure within which research is conducted; it constitutes the blueprint for the collection, measurement and analysis of data. As such
the design includes an outline of what the researcher will do from developing the initial questions of the study and how this is linked to the data to be collected and conclusions drawn (Edelson, 2002; AIS, 2007). This study will adopt the mixed method design. This will consist of survey and experimental designs. The first phase of the study will employ survey research design. The second phase will involve experimental design.

According to Kothari (2010), survey research design allows a researcher to explore and fully describe observed phenomena in this study this will be suitable for achievement of objectives one, two and three. This study intends to collect large amount of data and therefore survey research design is further preferred as it is suitable for collecting large amounts of data from large populations (Kothari, 2010). Surveys are appropriate for this research because the questions will explore self-reported beliefs or user behaviors (Neuman, 2007). They are strongest when answers people give to questions measure a certain variable.

The experimental research design will entail the researcher observing the users efficiency of use and the effectiveness of the employed biometric security technologies. The biometric traits that will be established from data emanating from this observation and data from the survey in objective 1 and 2 will then be consolidated and be used to design the prototype. The prototype will then be validated for use using an assessment tool as indicated in objective 4. This prototype will act as a model for identity authentication in organizations. This is in view that best end products are only gotten when the researcher anticipates real user scenarios from the prototyping phase (Cao, 2015).

3.4 Research Site

The geographical location of this research study will be in Nairobi, Kenya. Nairobi is purposively selected as a suitable study site because insecurity, organizational infiltration and terror threats have become so rampant (UNEP, 2012). Also Nairobi features most organizations that have employed biometric technologies. Furthermore, in this city most organizations are suffering from data integrity issues and require good and stricter authentication methods for anyone to access their data.
3.5 Target Population

The study population refers to the subjects under study (Cooper & Schindler, 2001). This study will target private organizations that have currently employed the use of biometric technologies. These organizations will be those that are using at least one biometric technology for authentication. This is because data collected from these organizations will be of relevance to the objectives of the study. At organization level, the study targets persons-in-charge of BSS in the organization as well as the users.

3.6 Sampling

Sampling is a process of selecting individuals from a population such that the selected group contains elements representative of the characteristics found in the target population (Kombo & Orodho, 2003). These sentiments are supported by Mugenda and Mugenda (2003), who state that a sample is a small group obtained from the accessible population as a representative of the entire population. Sampling will therefore be used to select organizations where this study will be carried out, as well as the respondents in these organizations.

3.6.1 Sampling Techniques

Purposive sampling will be used to identify the first private organization(s) that will provide a starting point for snowball. This study will use snowball sampling to identify specific organizations that have implemented desired biometric security technologies (BSS). This technique is appropriate given that many private organizations do employ authentication systems, but very few (usually unknown) utilize biometric security technologies. In this study, organizations of interest are difficult to locate hence snowball is applicable as it is a non-probability sampling technique that is appropriate to use when a study has such members of a population (Crossman, 2016).

By identifying few initial private organizations that use BSS the researcher will then proceed by snowball thus allowing these initial organizations to recommend other organizations that use BSS systems. To minimize on sample biasness, where a sampled organization refers the researcher to more than one other organization, simple random
sampling will be used to identify to which organization the study should proceed.

At organization level, the study will use purposive sampling to identify members with unique knowledge on BST that exist in their particular organization. These individuals will be persons-in-charge of BSS. The researcher will then use simple random sampling to select BSS users in these organizations for purposes of obtaining data on the factors influencing adoption and the usage of BSS.

### 3.6.2 Sample Size

Snowball sampling being a non-probability sampling method, the size of the sample is usually a sample ratio of size of the population (Blaikie, 2003). In this study, the overall population size is unknown due to lack of official statistical data in regard to private organizations that use biometric security systems. Faced with this challenge, the study will not base its sample size on mathematical theory for determining the sample size (Blaikie, 2003). The study will select cases gradually as the study progresses during data collection. For snowball, a sufficient sample size is believed to have been gathered when organizations start referring the researcher back to already sampled organizations.

### 3.7 Research Instruments

The instruments for data collection in this study will be questionnaires, interview schedules, observational schedules, document analysis tool and a prototype.

#### 3.7.1 Questionnaire

Questionnaires will be used for this study because they are free from the bias of the researcher thus they offer respondents time to provide well thought out answers. They are also mainly handy especially in cases where the respondents are not easily approachable and the samples are large. There will be one set of questionnaire administered to the employees in the selected organizations who will make up the sample.
The questionnaire will consist of a set of questions printed and arranged in a definite order on a form (Kothari, 2010). This questionnaire will be designed basing on previous research work as well as the objectives of the study and it will consist of structured questions to capture quantitative data. The questionnaire will contain two sections: a section for capturing the demographic information of the BSS user and another section that will attempt to quantify the characteristics of the BSS users.

A 5-point likert scale will be used to provide the users with the opportunity to rate their usage of BSS in their organizations. The 5-point likert scale offers flexibility, thus enables the respondents to express their opinion more precisely. Previous studies in biometric security systems have also used 5-point likert scale in their measurement of BSS performance (Lease, 2005; Patrick, 2016). The 5-point likert scale will contain the following points: strongly disagree, disagree, not decided, agree and strongly agree, which will be assigned values of 1, 2, 3, 4 and 5 respectively.

3.7.2 Interview Schedule

Interview, as a method of data collection involves presentation of oral or verbal stimuli and reply in terms of oral or verbal responses (Kothari, 2004), will be conducted in this study with persons-in-charge of BSS in participating organizations. A face-to-face, structured interview will be intended to last for duration of 20 minutes with the interviewee. Interviews will be used as a data collection instrument as they will enable the researcher deduce how consistent the responses from the questionnaires will be and to seek for clarity on certain questions. This will enable triangulation of gathered data.

3.7.3 Observation Schedules

Observation technique will be utilized to facilitate the achievement of objective three. Observation is a way of gathering data by watching behavior, events, or noting physical characteristics in their natural setting. This study will utilize observing-participant approach where the observer does not take part in the activities that are being observed (Colorado State University, 2016). It will utilize the advantages of covert observation where the participants being observed are unaware that they are being observed (Kawulich, 2005).
By being covert the research aims to not influence the behaviour of BSS users. The researcher will observe behavioural traits of the BSS users. This will involve observation of the biometric technologies and the data obtained will be used to design the architecture for the model (Kawulich, 2005). This architecture will be used as an input in the prototyping phase.

The observation schedule (see Appendix III) consists of a section for the BST that are intended to be observed. For each BST several characteristics will be considered for measurement then a remark based on the observed characteristic will be deduced.

### 3.7.4 Document Analysis

Document analysis tool provides a stable and reviewable way of collecting data (Yin, 2014). This study intends to analyze records of interest to the study that exist in the targeted private organization. These records include those containing general firm’s information, relevant information on biometric security and usability. Such records include: BSS evaluation reports, and efficiency of performance reports.

### 3.7.5 Prototyping

A prototype is an early sample, model, or release of a product built to test a concept, process or to act as an artifact to be replicated or learned from (Yogesh, 2006). According to Kendall & Kendall 2006, it is a term used in a variety of contexts, including: semantics, design, electronics, and software programming. This study will develop a prototype to enable the design of the MBSS model. This prototype is an important tool as it serves to provide specifications for a real, working system rather than a theoretical one. It was chosen for this research because it will be a superb way to elicit feedback about the proposed model and about how readily it will fulfill the information needs of the user as well as the organization.
3.8 Quality Control of Research Instruments

This is a precaution taken by the researcher to ensure that the research instruments are valid and reliable (Yogesh, 2006).

3.8.1 Validity of the Research Instruments

Validity of a test is a measure of how well a test measures what it is expected to measure (Kombo, 2006). This study will use face, content and construct validity to determine the validity of the research tools. Content validity will be achieved when the questionnaires will be pre-tested on a set of respondents especially those knowledgeable in biometrics.

This will enable the researcher to review the questionnaire items based on the pilot respondents. Face validity will be achieved through a panel of experts who will judge the survey tools based on the appearance, relevance and the representativeness of its elements (Burton & Mazerolle, 2011). Construct validity of the tools will be assessed by university experts and by use of standardized measures of BSS performance. The model to be designed will be validated using the tool to be developed to ascertain if it meets the specified requirements.

3.8.2 Reliability of the Research Instruments

Reliability is the measure of how accurate and precise an instrument or measurement procedure is (Kothari, 2010). It means that the instrument used is stable and will collect the same data if used in other similar studies. Reliability test will ensure that there is no ambiguity in the questions and those tools of data collection serve the intended purpose. In order to test for internal consistence of these tools, Cronbach’s alpha coefficient will be used as a measure of this reliability (IDRE, 2016). According to Santos, (1999) when the Cronbach alpha coefficient is greater than 0.7, the instrument is considered reliable. Questions set items that will indicate an alpha of less than 0.5 will be reviewed in order to raise the co-efficient.

This study will rely on a pilot study to test for content validity of the instruments. This will verify the reliability of the questionnaires to be used. Both equivalence and stability aspects of the research instruments will be verified from the analysis of data emanating
from the pilot study. This will provide a forehand opportunity to examine effectiveness of the instrument to be administered to the target population (Orodho, 2005). This pilot study will be conducted in Finlay Flower Company in Naivasha. This private company implemented the Biometric Security Technologies in 2012 and has used it for the past four years and has been using it successfully (Blaikie, 2003). It is also among the few private organization known for BSS use outside the targeted study area.

3.9 Data Analysis

After data has been collected, it will be edited organized and coded into SPSS software for analysis thereafter data will be analyzed using descriptive statistics as well as inferential statistics. The results will be tabulated, the information structured in order so that it can be easily and effectively communicated. Table 3.1 below gives a summary of the data analysis procedure:

**Table 3.1 Data Analysis Summary, Source Author**

<table>
<thead>
<tr>
<th>Objective</th>
<th>Data type (collected)</th>
<th>Statistical analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Quantitative</td>
<td>Descriptive: Mean, Mode, Frequencies and percentages</td>
</tr>
<tr>
<td>2</td>
<td>Quantitative and Qualitative</td>
<td>Descriptive: mean, mode, and median Inferential: Pearson product moment correlation</td>
</tr>
<tr>
<td>3</td>
<td>Quantitative</td>
<td>Descriptive: mean, mode, and median Inferential: Pearson product moment correlation</td>
</tr>
<tr>
<td>4</td>
<td>Quantitative and Qualitative</td>
<td>Descriptive: mean, mode, percentage Inferential: Pearson product moment correlation Inferential: Statistical modeling</td>
</tr>
</tbody>
</table>

The statistical analysis of this research will be:

Objective 1: Data on the types of BSS used in private organizations will be collected
using questionnaires, interviews and observations. Descriptive statistics will be computed to obtain a general understanding of the organizations using mean and mode. After the analysis this data will be presented by use of statistical techniques which include frequency distribution tables, percentages and graphs.

Objective 2: Data collected on this objective will be evaluated and the results will be used to form the major inputs that will be considered when designing the model for adoption of multimodal biometric security systems. Descriptive and Inferential statistics will be used. Correlation to test the relationship between the independent and dependent variables and factor analysis such as principle component analysis will be used to determine the contribution of the independent variable on the dependent variable.

Objective 3: For this objective data will be collected on the organizational factors influencing the adoption of biometric security systems through the use of questionnaires and interviews. Both descriptive and inferential statistics will be used. Descriptive statistics thus, mean, mode, and median will be computed. Inferential statistics will include a Pearson Product Moment Correlation to determine the influences of variables on each other.

Objective 4: the results from objectives 1, 2 and 3 will be used to design and develop a tool for validating the model. As such, the results of objectives 1, 2 and 3 will provide data that will be the input values for objective four.

3.10 Ethical Consideration

The research proposal will be submitted and approved by the school of graduate studies (SGS) and the Senate of Kibabii University (KIBU). The researcher will then proceed to acquire a research permit from the National Commission of Science, Technology and Innovation (NACOSTI) before proceeding to collect data. The questionnaires to be used in the study will be accompanied by a signed introductory letter to give a brief explanation of the purpose of the study. Before carrying out the interview, the researcher will seek the consent of the participants and will clearly explain to them the purpose of the interview also pointing out clearly that the information obtained will be handled
discretely and will be used for academic purposes only. All the materials used in the study will be properly cited and referenced.

3.11 Chapter Summary

A philosophical approach of this study will mainly be pragmatism because of the flexibility it will offer to the study. Mixed methods research design will be used on private organizations in Nairobi town. Purposive and snowball sampling techniques will be used to select participants of the study. The research instruments will be questionnaires, interviews, document analysis, observation schedules and prototyping. Before data collection exercise the research questions will be tested for reliability and validity. Data analysis will take both descriptive and inferential dimensions. Ethical issues will be considered and the necessary protocols will be followed.
REFERENCES


Behavioral characteristics: London, Sage

Ajzen, I., 1985. From intentionsto actions : a theory of planned behaviour,
Action Control: From Cognition to Behaviour.

Behaviour and Human Decision Processes


Ajzen, I., and Fishbein, M., 1980. Understanding attitudes and predicting social
behaviour. Prentice Hall.

International Symposium on Information Technology 1, 1-8


Capitalism. Frankfurt am Main: Peter Lang.

Al-Mamary, Yaser H., Alina S., and Nor A. (2014) "Factors Affecting Successful
Adoption of Management Information Systems in Organizations towards
Enhancing Organizational Performance." American Journal of Systems and
Alyson, J. K. (2012). *More than a military challenge; building a cooperative, security community.* University of Iceland


Anwar, S., A. (2013). *The criteria for effectiveness management practices among organizations.* Pearson international, New Delhi, India


http://blogs.ittoolbox.com/supplychain/eprocurement/procurementstrategy-key-to-successful-eprocurement-5125


Blaikie, N. (2003). Analysing Quantitative Data; *From Description to Explanation:* SAGE Publication LTD.


Colorado State University. (2016). Steps and methods used in qualitative observational research. Retrieved July 20, 2016, from Writing@CSU: writing.colostate.edu/guides/page.cfm?guid=11354&guidedid=63


level fusion in Multimodal Biometrics System, Proceedings of ABVPA,


Holt, K., L. (2012). *Achieving overall organizational success through technology- the


Manoj G., (2003). Biometric Technologies Overview, SANS Reading Room,


Odunga W (2012). Kenyan banking sector management programs and reforms; managing through technology, Rongo University Press, Rongo, Kenya


No. 5.


Tsou, A. Kokolakis, S. Lambrinoudakis, C. and Gritzalis, S. (2010)."A security standards' framework to facilitate best practices' awareness and


APPENDICES

Appendix I: Questionnaire

Introduction

I am a student pursuing a PhD in Information Technology from Kibabii University. I am carrying out research on “A Model for Adoption of Multimodal Biometric Security Systems in Private Organizations”. I will be grateful if you could spare a few minutes to complete this questionnaire on the adoption of a multimodal biometric security system in organizations. The researcher wishes to inform you that the information, views and opinions you divulge here will be kept confidential. Thank you most sincerely in advance for your cooperation.

Instructions

This questionnaire constitutes of three sections I, II, and III.

Please put a tick mark [✓] in the appropriate box whenever required

SECTION I: DEMOGRAPHIC INFORMATION

1). Background Information

a) Gender: Male [ ] Female [ ]

b) To which age group do you belong

   Less than 25[ ]  25-30 [ ]  31-35[ ]  36-40 [ ]  41-50 [ ]  Above 50[ ]

c) What best describes the work you do?

   …………………………………………………………………………………………………………

d) How long have you worked in this organization?

   0-4 years [ ]  5-9 years [ ]  10-14 years [ ]  15-19 years [ ] over 20 years [ ]

e) Please tick your highest academic qualifications

   i) Post Graduate [ ]
   ii) Degree [ ]
   iii) Diploma [ ]
   iv) Certificate [ ]
   v) Secondary School [ ]
   vi) Primary School [ ]
SECTION II: Type of Biometric Security Systems

a) How easy is it for you to use biometric security systems?

Very easy [ ]   Easy [ ]   Moderate [ ]   Difficult [ ]   Very Difficult [ ]

b) Identify the Biometric Technologies that you do use in your organization

i. Fingerprint [ ]
ii. Signature [ ]
iii. Hand Geometry [ ]
iv. Face Geometry [ ]
v. Iris [ ]
vi. Any other ..................................................

SECTION III: Biometric Security Systems

Please circle the appropriate number, for example 〇, so as to indicate the level of your agreement or disagreement with the following statements on a scale of 1 to 5, where 1= completely disagree, 2=slightly disagree, 3=neutral (You neither agree or disagree), 4=slightly agree, 5= strongly agree

<table>
<thead>
<tr>
<th>ITEMS</th>
<th>RESPONSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. I believe the Biometric Security Systems (BSS) is relevant and needed in this organization.</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>2. I believe the BSS has the ability to serve all members in this organization.</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>3. I believe the BSS gives us a good service as a system.</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>4. Whenever I access the BSS, it does not cause delays in processing my information.</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>5. I can easily reach the BSS to get my access permission.</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>6. The BSS is flexible enough to accept my data and give me the right output.</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>7. At times when I try to access the BSS, it</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td></td>
<td>generates false information</td>
</tr>
<tr>
<td>---</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>8.</td>
<td>Sometimes the BSS fails, thus it does not work.</td>
</tr>
<tr>
<td>9.</td>
<td>The BSS is simple and easy to use.</td>
</tr>
<tr>
<td>10.</td>
<td>I believe I am motivated to use the BSS</td>
</tr>
<tr>
<td>11.</td>
<td>I believe I have enough experience in using BSS</td>
</tr>
<tr>
<td>12.</td>
<td>I feel that the organization puts too much pressure on us to use the BSS</td>
</tr>
<tr>
<td>13.</td>
<td>I believe the use of BSS in this organization is a good thing.</td>
</tr>
<tr>
<td>14.</td>
<td>The management support the use of BSS.</td>
</tr>
<tr>
<td>15.</td>
<td>I believe this organization is or was not technologically ready to use the BSS.</td>
</tr>
<tr>
<td>16.</td>
<td>A specific person is always available to help with any difficulty encountered when using the biometric security system</td>
</tr>
<tr>
<td>17.</td>
<td>The BSS used in this organization receive sufficient technical support.</td>
</tr>
<tr>
<td>18.</td>
<td>This organization has necessary resources to enable the use of biometric security systems.</td>
</tr>
<tr>
<td>19.</td>
<td>This BSS has been integrated into other departments/sections in this organization.</td>
</tr>
<tr>
<td>20.</td>
<td>This BSS is integrated in our other organizations elsewhere in the country.</td>
</tr>
<tr>
<td>21.</td>
<td>I believe there are additional benefits to an organization using BSS.</td>
</tr>
<tr>
<td>22.</td>
<td>Using biometric security systems enhances confidence in me so I perform my job with ease.</td>
</tr>
</tbody>
</table>
THANK YOU FOR YOUR TIME
Appendix II

Interview Schedule

Interview schedule for persons in charge of Biometric Security Systems

The purpose of this interview is to gain insight on the adoption of biometric security systems in private organizations. The researcher is a student of Kibabii University undertaking a Doctor of Philosophy in Information Technology. Information gathered through this interview will be solely used for the purpose of this study.

Kindly spare sometime and provide the researcher with accurate information.

1) For how long have you served in this organization?

2) Which biometric technology (ies) have been adopted in this organization and for how long?

3) In your own opinion, are the Biometric Security Technologies implemented in this organization effective as authentication methods? (performance, uptime, technical support, reliability)

4) At your organization, what would you say about the reception of BSS usage, was it well received or not? If Yes explain why? If No explain why?

5) What challenges have you experienced as a result of adoption and effective use of biometric security systems in your organization with reference to:
   i. Improving service delivery?
   ii. Improving security?
   iii. Recognition performance?

6) What measures have you put in place to overcome these challenges and support biometric security system adoption and use?

7) Do you have a biometric security system adoption policy in your organization?
   a. If yes is it implemented and currently in use?

8) What recommendations would you like to make in relation to the problem of adoption and effective use of biometric security systems by organizations?
9) Were there partnerships in the implementation of the biometric security systems in your organization? Yes [ ] No [ ]
   If yes state them .................................................................

THANK YOU
Appendix III

Observation Guide

Organization code: __________

1. Types of Biometric Security Systems in the Organization

<table>
<thead>
<tr>
<th>S/N</th>
<th>Characteristics</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Unimodal</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Multimodal</td>
<td></td>
</tr>
</tbody>
</table>

2. How effective are the existing Biometric Security Technologies in the organization

<table>
<thead>
<tr>
<th></th>
<th>Fingerprint</th>
<th>Signature</th>
<th>Hand Geometry</th>
<th>Face Geometry</th>
<th>Iris</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ease of use</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reliability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accuracy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Runtime</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Robust</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. What is the recognition performance of the implemented Biometric Security Technologies in the organization

<table>
<thead>
<tr>
<th></th>
<th>Fingerprint</th>
<th>Signature</th>
<th>Hand Geometry</th>
<th>Face Geometry</th>
<th>Iris</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FAR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FRR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix IV

Document Analysis

<table>
<thead>
<tr>
<th>Information</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>i) The age of the private organization</td>
<td></td>
</tr>
<tr>
<td>ii) Organizational structure</td>
<td></td>
</tr>
<tr>
<td>iii) Number of Branches across the country</td>
<td></td>
</tr>
<tr>
<td>iv) Number of employees in the private organization</td>
<td></td>
</tr>
<tr>
<td>v) Type of BSS in place</td>
<td></td>
</tr>
<tr>
<td>vi) Biometric technology employed</td>
<td></td>
</tr>
</tbody>
</table>
Appendix V

Prototyping Plan

- Data collected from objective 1
- Data collected from objective 3

Identified Preferred Biometric Technologies after analysis

- Requirement Specification
- System Design (Architecture)
- Prototype Construction

Figure 3.1 The Prototyping Plan
Appendix VI

Schedule

The study will be carried out within the time plan as shown below

<table>
<thead>
<tr>
<th>Activity</th>
<th>Year 1 (Quarters)</th>
<th>Year 2 (Quarters)</th>
<th>Year 3 (Quarters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Course Work, Proposal defense,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2 Literature review, Research design</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3 Developing &amp; Validating Tools</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.4 Data Collection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5 Data Analysis</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.6 Designing the Biometric</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.7 Documentation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.8 Thesis Presentation and Defense</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Appendix VII

### Budget

#### Yearly itemized budget (Ksh)

<table>
<thead>
<tr>
<th>a). Expendable supplies</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometric SDK (Software for Biometric Integration e.g. M2SYS)</td>
<td>40,000</td>
<td>80,000</td>
<td></td>
</tr>
<tr>
<td>Software (middleware e.g. OS)</td>
<td>20,000</td>
<td>15,000</td>
<td></td>
</tr>
<tr>
<td>Biometric Scanners</td>
<td>80,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Journals and literature research</td>
<td>15,000</td>
<td>30,000</td>
<td></td>
</tr>
<tr>
<td><strong>Sub-total</strong></td>
<td><strong>75,000</strong></td>
<td><strong>205,000</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>b). Item Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometric Application Server (BioSP)</td>
<td>250,000</td>
</tr>
<tr>
<td>Costs for coding for tool</td>
<td>50,000</td>
</tr>
<tr>
<td><strong>Sub-total</strong></td>
<td><strong>250,000</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>c). Documentation and publication costs</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation</td>
<td>5,000</td>
</tr>
<tr>
<td>Publications (papers in three refereed journals)</td>
<td>15,000</td>
</tr>
<tr>
<td>Publication of thesis</td>
<td>90,000</td>
</tr>
<tr>
<td><strong>Sub-total</strong></td>
<td><strong>20,000</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>d). Local travel</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Collection from Private institutions</td>
<td>15,000</td>
</tr>
<tr>
<td>Costs of meeting the officials to disseminate the findings</td>
<td>10,000</td>
</tr>
<tr>
<td>Travel to conferences, validation and tool patenting</td>
<td>10,000</td>
</tr>
<tr>
<td><strong>Sub-total</strong></td>
<td><strong>35,000</strong></td>
</tr>
<tr>
<td></td>
<td>Other costs</td>
</tr>
<tr>
<td>---</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>e)</td>
<td>Printing Costs</td>
</tr>
<tr>
<td></td>
<td>Patenting Costs (For the tool)</td>
</tr>
<tr>
<td>f)</td>
<td>Total Yearly budget</td>
</tr>
<tr>
<td>g)</td>
<td>TOTAL BUDGET</td>
</tr>
</tbody>
</table>