BIOMETRIC AUTHENTICATION SYSTEMS AND SERVICE DELIVERY IN HEALTHCARE SECTOR IN KENYA

MULUMBA, MARTHA ADILA

D61/P/7133/03

A MANAGEMENT RESEARCH PROJECT SUBMITTED IN PARTIAL FULFULLMENT OF THE REQUIREMENT FOR AWARD OF MASTERS OF BUSINESS ADMINISTRATION (MBA), SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

NOVEMBER 2012

DECLARATION

This project is my original work and has not been submitted for a degree in any University.

Signed ____________________ Date _______________________

MARTHA ADILA MULUMBA

This research project has been submitted for examination with my approval as a University Supervisor

Signed ______________________ Date _______________________

JAMES T. KARIUKI

Lecturer, Department of Management Science

School of Business

University of Nairobi

ACKNOWLEDGEMENTS

I am grateful to my family for affording me the time to undertake my MBA studies. Special thanks go to my husband Kyalo and to my friend Nyambura for their overwhelming support, understanding and encouragement.

Thanks to my supervisor, Mr. J. T. Kariuki for his guidance, which was a major contributor to successful completion of this project.

Gratitude to all the respondents of my questionnaires, this piece of work could not be completed without your invaluable contribution.

DEDICATION

To Kyalo, Vinya and Sila

ABSTRACT

Biometrics is the automated method of recognizing a person based on a physiological or behavioural characteristic. Although biometric is a technology that has been surrounded by a number of issues, the advantages associate with it has seen its deployment across sectors. In Kenya, the largest deployment witnessed so far has been in the healthcare sector. However, there is limited literature on the performance of biometrics in healthcare sector and its impact on service delivery.

This study constituted a descriptive survey involving 43 healthcare facilities that were using biometric systems within Nairobi city in Kenya. The study objective was to look at the factors affecting the performance of biometrics in the healthcare sector and the impact of its use in service delivery.

The findings revealed a number of factors affecting the performance of biometric systems in the healthcare facilities which include system response time, technical accuracy, ease to operate, information output, security, knowledge of biometrics by the IT support, IT support willingness to help, ability to withstand large number of users, system ease of use by patients, system user experience, reliability, promptness of IT support team and patients manner of usage.

The study identified efficiency in service delivery, reduction of financial losses, convenience, and customer satisfaction as the positive impact of the system while service denial and hindrance to excellent service delivery were identified as the negative impacts.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

APHIA	AIDS, Population and Health Integrated Assistance
BioAPI	Biometric Application Programming Interface
CBEFF	Common Biometric Exchange File Format
DNA	Deoxyribonucleic Acid
FAR	False Acceptance Rate
FBO	Faith Based Organization
FRR	False Rejection Rate
FTE	Failure to Enrol
HIPA	Health Information Protection Act
HIS	Health Information Systems
IEBC	Electoral and Boundary Commission
IIEC	Interim Independent Electoral Commission
IT	Information Technology
M&L	DeLone and McLean
NCAPD	National Coordinating Agency for Population and Development
NGO	Non-Governmental Organization
UAP	Union and Provincial Insurance
SPSS	Statistical Package for the Social Sciences

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

There have been massive innovations in healthcare sector over the past decade with the aim of enhancing health care procedures, cost effectiveness as well as efficiency (Omachonu and Einsprunch, 2010). Information technology (IT) has played a vital role in these innovations and has seen the emergence of biometric authentication systems in healthcare. The application of biometric technology in healthcare has been mainly prompted by security concerns, in the areas of medical schemes and patients' medical records ("Biometrics in Healthcare", 2009.).

Biometrics refers to a science involving statistical analysis of biological characteristics (Zhang, 2000) and represents the measurement of physiological or behavioural characteristic that is distinctive to an individual (Jain, Hong & Pankanti, 2000) such as face, fingerprint, palm print, retinal scan, iris pattern, keystroke dynamics, signature, and voice pattern. Biometrics is considered a definitive and superior method in authentication and identification of individuals (Heracleous and Wirtz, 2006). A biometric authentication system is a pattern recognition system that validates a person's identity by comparing captured biometric data with an existing biometric template(s) stored in a database (Jain, Ross, and Prabhakar, 2004).

Biometrics technology has been surrounded by a number of technical, social and legal issues which have impacted on its growth. Like most emerging technologies, biometrics has been subjected to high performance expectations and some systems have proven inadequate when assessed using a combination of factors such as; system error rates, robustness, usability, user acceptance and security (Pato and Millett, 2011). The technical performance in terms of accuracy and speed of recognition is key to successful implementation of biometric systems (Jain et al, 2004). The fact that there is no biometric system that is free of recognition errors has been a major challenge. Systems have failed due to technical inefficiencies. For instance, a Malaysian border checkpoint biometric system failed the speed test leading to lost business as tourists cancelled their visits (Homeland Security News Wire, 2011). It is such performance failures that have led to resistance by number of potential users as the perceived and portrayed inadequacies may lead to adverse effects on services delivery and to the entire business.

Regardless of the area and scope of application, the impact of biometric systems has been noted to be diverse with both positive and negative outcomes (European Community, 2005). The impact of biometrics in service delivery relate to efficiency and convenience of transactions, costs of and savings in service delivery, security and safety of individuals and resources, and in customer satisfaction (Jain et al, 2004; Pato and Millett, 2011).

Notwithstanding identified challenges, biometrics seems to be gaining popularity in Kenya. The trend towards acceptance can be demonstrated by increased implementations of the biometric systems by a number of players in different sectors. In Kenya, limited applications have been seen in banks' back offices and in retail stores, for physical and system access control. The Independent Electoral and Boundary Commission (IEBC) of Kenya previously Interim Independent Electoral Commission (IIEC) has already piloted a biometric voter registration and verification system, which is supposed to be rolled out in the whole country (Neurotechnology, 2011). The healthcare sector has not been left behind in this, but unlike the banks and retail chains where the applications have been limited to the use by employees only, the healthcare providers are using biometrics to authenticate their clients.

1.1.1 Kenyan Healthcare Sector

The healthcare in Kenya can be categorized into two broad categories; the public sector and the private sector. The private sector includes private for-profit, Non-Governmental Organization (NGO), and Faith Based Organization (FBO) facilities (Muga, Kizito, Mbayah & Gakuruh, 2004). Health services are provided through more than 8,211 health facilities countrywide, with the public sector system accounting for about 46% of these facilities. The distribution of the healthcare facilities in Kenya by province is as depicted in Table 1 (Ministry of Public Health and Sanitation and the Ministry of Medical Services, 2012).

Table 1.1: Healthcare Facility Distribution by Province

Province	Total
1. Central	1439
2. Coast	870
3. Eastern	1477
4. Nairobi	534
5. North Eastern	287
6. Nyanza	954
7. Rift Valley	2128
8. Western	522
Grand Total	**8211**

Source: Ministry of Public Health and Sanitation and the Ministry of Medical Services, 2012

The sector has been characterized by disparities in the distribution of health services, resource allocations, and unequal access to quality health services (Ndavi, Ogola, Kizito, and Johnson, 2009). The public health system consists of national referral hospitals, provincial general hospitals, district hospitals, health centres, and dispensaries with the well-equipped facilities concentrated in the urban areas. The private health sector has a similar structure with a small number of large private providers that offer high-quality services concentrated mainly in Nairobi, Kisumu, and Mombasa and small-scale providers located throughout the country (Barnes, et al, 2010).

In effort to alleviate the healthcare services disparities, the government of Kenya has put in place strategies which when fully implemented are supposed to improve healthcare provision. Among them is the Strategic Plan for Health Information Systems (HIS) which guides the implementation of countrywide HIS aimed at improving service delivery to Kenyans (Ministry of Health & Ministry of Public Health, 2009). The private healthcare sector is ahead of the public sector in the implementation and use of HISs as they content with the competition in the sector. The HISs are aimed at achieving better management of information, tighter controls of resources, and better patient care (AIDS, Population and Health Integrated Assistance (APHIA), 2001). The latest notable HIS innovation in the healthcare sector is the biometrics authentication system.

1.1.3 Biometrics application in Kenyan Healthcare

The Kenyan healthcare like the rest of the world have realized the cost benefits of biometrics systems when compared to the cost of medical benefits fraud, the cost of fraud prevention and the cost of mistakes that can be prevented by use of biometrics (“Biometrics in Healthcare”, 2009). Despite numerous reasons of biometric application, medical scheme frauds can be singled out as the driving force behind biometrics in the Kenyan healthcare sector (Iselin, 2010). It is estimated that in the year 2009, fraud in the medical insurance sector caused revenue losses estimated at 40 per cent of total claims (Mbogo, 2011). Medical insurances and companies, in partnership with healthcare providers have introduced biometric authentication systems to counter this problem. The solution is designed to prevent and deter medical benefits over expenditure, sharing of medical benefits with non-members, payment of services not rendered among other misuse of medical insurance.

Subscribers to a number of medical insurances and employees of some companies, among them Standard Chartered, Barclays Bank Kenya, Union and Provincial Insurance (UAP), AON Minet and Jubilee (Iselin, 2010) are issued with smart cards in which their biometric data is stored. At the time of service, the cards are inserted into a reader and the subscriber places fingers on a biometric scanner that verifies the identity as well as benefits entitlement for the subscriber.

According to Iselin (2010), the use of the smart cards in healthcare is gradually increasing as in March 2010 there were already 150,000 smart cards issued out and there were more than 1000 points of service countrywide. More cards have been ordered from the supplier since then (ThirdFactor, 2011).

1.2 Statement of the Problem

Although commercial applications are emerging there are still concerns on biometric system performance, especially in large-scale application (Chandra and Calderon, 2005). While biometric technology is used in a variety of applications, questions remain regarding the technical and operational effectiveness of biometric technologies (Rhodes, 2003).

However, it is argued that technological improvements have contributed in making biometrics solutions more viable, less expensive and more accurate, leading to increased acceptance by potential users (Coats et al, 2007). According to Heracleous and Wirtz (2005), if the power of biometrics is exploited, it shall be the next technology after the Internet to enable value and productivity enhancements. Heracleous and Wirtz, (2006) further suggest that biometrics can offer significant security enhancements as well as other value-added applications including improvement in service delivery.

Despite performance concerns and uncertainties surrounding the technology, organizations in Kenya like elsewhere continue to implement biometrics. Substantial amount of money is being invested in the technology yet the capability of the systems to handle large number of users in a large-scale application is uncertain.

While the potential of biometrics has been acknowledged, doubts have been cast on whether the system implementations are unlocking the full benefits of the system. There are claims that the benefits of biometrics are unattainable due to a number of barriers (Grijpink, 2004). The success or failure of biometrics system is dependent on a number of factors and the area of application. The benefits realization, limitations and factors that affect the performance of the systems in healthcare sector have not been highlighted.

Biometrics being a new phenomenon in Kenya, little research work has been done on the subject. Although a number of studies have been undertaken on different areas of biometrics and healthcare service delivery, there is none that has been focused on the impact of biometrics in healthcare service delivery. A survey by Abanti (2010) aimed at determining the acceptability of biometric-based authentication system in a private university in Kenya and among his recommendations was further research to examine the effects of biometric authentication systems on the efficiency and speed of existing hardware. Owiti (2010) explored the factors affecting the acceptance of mobile phone technology in the delivery of healthcare services. Kariuki (2010) focused on challenges faced by Medical institutions in procurement, implementation and maintenance of information and communication technology (ICT). Further, biometrics applications have been more focused on solving security problems without emphasis on the impacts the systems have on services (Neurotechnology, 2011, Heracleous and Wirtz, 2006).

Given the use of biometric authentication systems in Kenyan healthcare facilities, the study aimed at determining the impact of these systems on service delivery. The research sought to answer the question: How does the use of biometric authentication systems impact on service delivery in healthcare facilities in Kenya?

1.3 Research Objectives

This research focused on the application of biometrics in healthcare facilities in Kenya. The objectives of the study were to:

1. Establish factors affecting the performance of biometric authentication systems used in healthcare facilities in Kenya.
2. Determine the impact of biometric authentication in service delivery.

1.4 Value of the Study

This research contributes to the existing knowledge on biometrics and shall provide reference material to scholars. The research recommendation is of importance to researchers, as it provides basis for further research work on other aspects of biometrics.

The findings from this study are beneficial to decision makers in Kenyan healthcare. They will be able to make informed decision regarding application of biometrics in healthcare. The study also provides feedback to those who are already using the technology. This is useful in future consideration of biometric application in different areas of healthcare.

The study is useful to stakeholder in the financial industry where the problem of identity fraud has been prevalent. The performance of biometrics on large scale and client base has been a concern as unfavourable effect may mean loss of business. Thus, findings of this study would assist in making decisions regarding biometric applications

The government of Kenya and its departments are in the process of implementing biometric systems in a number of areas. This research provides them with insights on the performance of the system on large population hence help shape their implementation plans.

System developers and solution provider also benefit from this research, as it informs them of experiences of the customers as well as the performance of the systems.
This will help them in their future biometrics solution designs.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

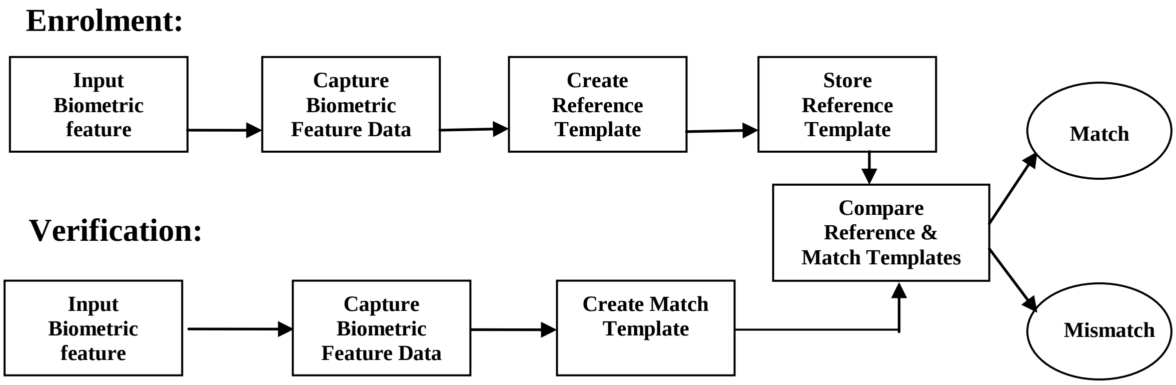
Biometrics is the automated method of recognizing a person based on a physiological or behavioural characteristic. According to Coats et al (2007) physiological characteristics are unique identifiers because no two people have identical biometric measurements. Physiological biometrics uses physical trait, such as a fingerprint, iris, hand or face for recognition while behavioural biometrics involves the use of a behaviour trait or pattern, such as a voice, signature or keystroke.

Authentication is the process of reliably verifying identity of an individual or something (Russ, 2000). It is the process of determining whether someone or something is, in fact, who or what it is declared to be. Biometric authentication refers to automated method of verifying the identity of a living person in real time based on physical characteristic or personal trait (Woodward et al 2001).

A biometric system can be either a verification (authentication) system or an identification system. Identification is the confirmation of one's identity using an identifier like username. Verification is confirmation or denial of an identity using a verifier like a password. In biometrics, verification involves authenticating users in conjunction with smart cards and usernames and this is called biometric authentication.

While biometric identification compares an individual's biometric templates with a set of many stored profiles and finds the best match, authentication involves a one-to-one matching of an individual's live reading and his or her stored profile (Ruggles, 2002). Identification answers the question "Who is this person" while authentication poses the question "Is this person who he or she claims to be?" Authentication is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity (Jain et al., 2004). Figure 1 below illustrates the authentication process.

Figure 2.1: The process of biometric authentication/verification



Source: Global Security

2.2 Biometrics System Performance

When evaluating the performance of an operational biometrics system with regard to service delivery, two perspectives can be assumed; technical and operational perspective. There are seven attributes of both physiological and behavioural traits that are crucial when designing a biometric system as they affect the overall performance of the system. (Jain et al, 2000: Zhang, 2000). These characteristics include universality, a characteristic possessed by every person; uniqueness, a characteristic that no two people share; permanence, a characteristic that is invariable with time; collectability, a characteristic that can be measured quantitatively; acceptability, a characteristic that is acceptable for usage by people; performance, a characteristic of achieving accuracy in identification and circumvention, the hardness of the system that prevents it from being cracked. Different types of biometric systems have different fulfilment of these seven attributes (Gamassi, et al, 2004). This results to variations when measuring human traits and behaviour hence affecting both technical and operational performance.

The technical performance of any given biometric system is usually gauged on three mathematically derived measurements that determine the matching accuracy of individual’s traits and the ability to enrol a user (Jain et al., 2000). During authentication the system performs a match between the existing template and the present template of an authenticating user. Take a case of user X trying to authenticate with own template. If the system fails to authenticate X, the system performs false rejection error and the probability of this happening is referred to as False Rejection

Rate (FRR). The lower the FRR, the less likely of one being falsely rejected by a system and the better the system performance. On the other hand, take case two of user X trying to authenticate as user Y. If the system matches user X’s template with that of Y, this is referred to as false acceptance error. The probability of this error happening is referred to as False Acceptance Rate (FAR). The lower the FAR, the less likelihood of a false match and the better the performance of the system. When one needs to enrol and the system does not allow enrolment, this is referred to as Failure to Enrol (FTE). The lower the FTE, the better the biometric system performance.

During the design phase of a biometric system, FRR and FAR tolerance is put into consideration in relation to system application area. This is crucial to system performance as it prevents frustration and fraud caused by false rejection and false acceptance respectively (Polemi, 1997). Frustrations would translate into customer dissatisfaction, both to internal and external customers of the system.

Speed at which the system processes request is another performance measure. In a client oriented service speed is a major determinant of customer satisfaction. The time required by the system to make authentication decision is critical especially in real-time transaction (Jain et al., 2000). System with minimal time requirement means faster and is be more acceptable to the users.

Two other related performance measure of a biometric system is the uniqueness and stability of the system. The stability of authentication outcome is highly desirable characteristic as variability in the biometric data submitted for comparison to the enrolled reference data can affect performance (Pato & Millett, 2011). The authentication outcome should be unique and shouldn’t change every time one undergoes the process. This would mean no requirement for other identification hence enhancing speed and acceptability by users

Convenience of use and accessibility are importance factor in determining the performance of a biometric system. Accessibility is to the ability of all types of users including the physically challenged to successfully access and use a biometric system (National Institute of Standards and Technology (NIST), 2008). The accessibility and ease of use affects the amount of time required for enrolment, identification or authentication and contributes to the speed of system transaction.

User acceptability is another dimension in measuring operational performance of a biometric system. This is driven by the user friendliness of the system. Some technologies are not socially acceptable as they don't satisfy user's security needs (Polemi, 1997). Non-intrusive systems are perceived as user-friendly as they don't come into conduct with individual's body (Jain et al, 2000). In some societies people are unwilling so use technologies that involve touching places where others have touched like in the case of fingerprints, hand geometry and vein recognition (Nelson, 2008). Lack of acceptability means the biometric devices are not used properly resulting to errors and more time spent on enrolment or authentication.

2.3 Advantages and Concerns of Biometrics

According to Emre (2000) proper design and implementation of biometric authentication system can indeed increase security. Biometrics provides increased security and it is so far considered the most secure means of identification and verification of individuals (Coats et al, 2007, Zhang, 2001). The use of smartcard based solutions is much more promising in security (Emre 2000).

Another advantage associated with biometrics is the accuracy that it provides (Coats et al, 2007). When the system is set up correctly, biological characteristics provide completely unique data sets that cannot be replicated easily. This makes it very difficult for anyone to forge someone else identity, therefore ensuring accuracy in authentication.

Biometrics eliminates problems caused by lost or forgotten passwords, burden on the users is reduced the as they do not have to remember passwords. Biometrics also prevents unauthorized use of lost or stolen ID cards and reduces password administration costs as well (Jain et al., 2004).

Minimum training is needed to get biometric system operational. Further, high-quality and well-implemented biometric systems require minimal maintenance, hence cutting costs (Schneider and Price, 2001).

Although biometrics promises greater security system (Matyas and Riha, 2003), user convenience and satisfaction (Jain et al., 2000), efficiency and cost effectiveness (Schneider and Price, 2001) among other benefits, biometrics is not without controversy. Biometrics has raised questions about personal privacy among the potential and current users. Biometric systems facilitate collection of varied wide range of data including individual’s movements, state of health and transactions carried out among others. There is the fear of information creep where an individual’s personal information find its way to a third party and utilized for purposes not intended for during collection. Issues of stealing and tampering of the biometric data is a challenge resulting to users distrust in biometric technology.

Grinjpink (2010) allude that the usage of biometrics may result to identity theft through stolen biometric data by hackers. Stolen biometric identifiers are likely to result to a greater loss as compared to stolen PINs, passwords or card since these can be revoked easily unlike biometrics. However, this claim ignores the fact that the data stored in biometric-based systems is an algorithm representation and not actual image of the identifier (Coats et al, 2007). In addition, some biometric systems do not store data in a central database, but on smartcards.

Standards for biometrics applications are lacking making biometric systems from different manufacturers incompatible (Berger, 2007). This has slowed down the adoption of biometrics as the adopters are not willing to invest in a system which is costly and that will change after a while (Lawson, 2003). However, with the emergency of Biometric Application Programming Interface (BioAPI) and the Common Biometric Exchange File Format (CBEFF) improvement in standards is expected. The BioAPI is designed to provide a cross-platform interface that simplifies development and standardizes programmatic interaction with biometric devices (Tilton, 2002). The CBEFF was developed to facilitate improved interoperability between biometrics systems and simplify hardware and software integration. As standards evolve and understanding of biometrics benefits grows, adoption of the technology is expected to grow exponentially (Chu & Rajendran, 2009).

There is concern with the health safety of the biometric devices. Users are afraid that device sensor may be harmful to human health and also infections due to use by large number of users (Biometrics News and Information, 2008). It should however be noted that, the sensors and other devices used for biometric analysis are based upon wimple digital technology which is harmless.

At least each of the current biometric systems have a portion of a small population that cannot enrol due to lack of biometric identifier like missing fingers or because of being unable to enrol (Rhodes, 2003). Others are falsely rejected by the system, while other identifiers just deteriorate with age (Jain et al., 2004). However the emergence of multi-biometric systems is a promising solution to this problem. Multi-biometric combines biometric traits for identification and verification. Apart from solving the problem of enrolment, it is considered to be better performer than single biometric system in terms of better security and efficiency.

As it is common with the adoption of any new system, there is general resistant to change. Due to may be religious beliefs, attitude and the criminal connotation associated with some biometric systems, users are bound to resist the adoption of these systems (Pooe and Labuschagne, 2009). The cooperation of the users especially for the intrusive systems is highly required otherwise they may not be able to enrol or match. This is however expected to change as users get to understand the benefits associate with the systems. User awareness campaigns and deployment of non-intrusive system may help improve acceptability (Giesing, 2003)

2.4 Biometrics Application in Healthcare

Biometrics is a rapidly evolving technology and a wide variety of competing biometrics solutions do exist in the market today. Biometric applications are now found in diverse fields including enterprise networks, homeland security, electronic and non-electronic banking, retail sales, law enforcement, healthcare and social services. Different types of biometric applications are suited for different areas of application.

Healthcare like others in the service industry have realised the benefits and the applicability of biometrics in the health sector. There are number of reasons why healthcare sector is turning to biometrics. Literature (Abanti, 2009, Wirtz and Hercleous, 2006) indicates that the main reason for biometrics adoption in healthcare worldwide is fraud, which is true in both developing and developed countries. Millions of dollars in medical scheme fraud are being lost every year and health care stakeholders have gone into biometrics in effort to prevent further loses. Healthcare facilities have been experiencing difficulties in patient verification and the use of biometrics is a promising solution (Jain et al., 2000). This has facilitated matching patients to their medical scheme benefits and preventing illegal sharing of medical benefits.

Contrary to the belief that biometrics may compromise on privacy; privacy of patients' records is a major driving force for biometrics in healthcare. With increased use of electronic records that are easily available compared to hard copies, countries are putting legislation in place to safeguard the privacy of patients. Biometric authentication is being used to control access to both electronic and hard copy medical records, thus ensuring individuals only access the records they are authorized to. Legislations like Health Information Protection Act (HIPA) in USA that imposes stringent requirements to protect patient privacy and the confidentiality of patient information (Schneider and Price, 2001) are pushing healthcare facilities to adopt biometrics to be in compliance with the new standards and requirements. Such legislations are having positive impact in the growth of biometric technology (Jain et al., 2000).

Another reason for biometrics in healthcare is risk management. Biometrics is facilitating risk management by ensuring patients identification is tied into care or treatment plans and matched to the right medical records (Schneider and Price, 2001). This is enhancing patient's safety and is being used in emergency case where the patients may not be in a position to identify themselves.

Resources management is another reason for implementing biometrics in health facilities. Biometrics in healthcare is being used to allow only authorized doctors and hospital staffs to access and use these certain medical equipment, drug stores and networks.

According to Li and Jain (2009), healthcare is turning to biometrics in order to balance convenience, security and compliance. Improving efficiency and compliance, reducing medical benefits fraud that is prevalent in this sector, restricting access to medical information and physical resources, and patient verification are the main reason for biometrics in healthcare.

A number of competing biometric technologies are in use and others under development. Considering that there is no one biometric technology that is 100% accurate (NSTC, 2006), there are a few that have done well and are commonly used in the healthcare applications. This is because different types of biometric system are more appropriate for certain contexts and operational purposes than others. Naturally the physiological biometrics has proved more reliable than the behavioural as the physical traits generally stay the same all the time, whilst the ever changing behavioural traits have more chance for error.

Fingerprint Recognition is probably the most popular among the biometric technologies (Pardesi, 2007) in all industries including healthcare. According to Schneider and Price (2001), fingerprints ultrasonic imaging is a breakthrough technology that delivers superior accuracy, speed, reliability and scalability for all healthcare biometric fingerprint identification applications. The fingerprints ultrasonic imaging technology has the ability to penetrate many materials and passes through contamination of the finger or the scanning devices. It is believed to improve accuracy in all population groups, including children and races. Early adopters of the fingerprint technology like Catholic Health in Buffalo, New York who have been using fingerprint authentication for their patients since 2003 ("Healthcare IT News", 2005) are a testimony of the success of the technology in healthcare. The same technology is in use in Angolan hospitals (M2SYS, 2010) and preliminary investigations indicate use in Kenyan healthcare facilities too. The negative side of the fingerprints technology is that it is considered intrusive and is feared to contact communicable diseases.

A relative new technology building on fingerprints weakness is the palm vein recognition. The vein technology is appealing in healthcare because users do not have to touch the scanner thus eliminating the risk of infection (Martin, 2007). Carolinas Healthcare is using this technology to identify patients during admission (Nelson, 2008). Their choice for this technology was driven by concerns of infection and wearing out of fingerprints scanners. According to Fujitsu (2005) vein recognition is high in accuracy with a false rejection rate of 0.01% and an insignificant false acceptance rate of less than 0.01.

Iris recognition is another biometric technology used in healthcare. It involves scanning and analysis of the iris of the eye using regular video camera. It is widely regarded as the most safe, accurate biometrics technology and capable of performing 1-to-many matches at extraordinarily high speeds, without sacrificing accuracy (Jia, 2005). Glasses or contact lenses rarely impede it. Iris recognition is a highly mature technology with a proven track record in a number of application areas. It has been used in University of South Alabama Hospitals (iHealthBeat, 2002) and City Hospital of Bad Reichenhall (Shoniregun and Crosier, 2008) for access control.

Iris recognition is considered better in terms of FAR compared to fingerprints. The iris patterns are stable over a lifetime as they are protected from damage by the cornea, and have six times as many distinguishable characteristics as a fingerprint (Ruggle, 2002). Other biometric technologies that have been applied in healthcare but in limited use include hand geometry, retina scan and Deoxyribonucleic Acid (DNA).

Though a number of biometric modalities have done well in healthcare application, there are cases where they have failed. An example case is the Eagleville hospital in Pennsylvania where they had to do away with iris recognition system due to inefficiencies (Martin, 2007). According to Pato and Millett (2011), failure of biometric systems is not necessary cause by the technology applied but due to a number of factors related to planning and implementation. These factors include inappropriate technology choices, lack of sensitivity to user perceptions and requirements, presumption of a problem that does not exist, inadequate surrounding support processes and infrastructure, inappropriate application of biometrics where other technologies would better solve the problem, lack of a viable business case, and poor understanding of population issues, such as variability among those to be authenticated or identified among others.

2.5 Impact of Biometrics in Healthcare

Success or failure of biometric systems determines the impacts they have on delivery of service. Biometrics is associated with operational efficiencies for identification and verification procedures (Schneider and Price, 2001). According to Bataller (2011) biometrics enables self-service and automated authentication of individuals, therefore improving operational efficiency while assuring security. Successful biometric systems implementation with high accuracy in recognition improves efficiency by shortening patients' registration process through automatic identification and insurance eligibility verification. This can lead to reduced overall waiting time for the patient which is critical to ensuring safe and expedited treatment (M2SYS, 2010). Biometrics has the potential to improve customer service and enhance customer satisfaction across industries (Wirtz and Hercleous, 2006). Efficiency in service contributes to improved customer satisfaction (Jain et al., 2000). In addition staff productivity is increased as one staff can serve more people within short time.

On the other hand, if the processes to use biometrics are lengthy or erroneous due to system inefficiencies, the ability of delivering services to the customers could be negatively affected. This would translate to long queues resulting to frustration both to the patients and staff. This would further lead to reluctance in use of the system by both patients and staff culminating to abandonment of the system.

Medical benefits fraud is one of the main reasons for biometrics in healthcare. Biometrics is capable of reducing fraud by verifying the identity of recipients at service delivery points thus reducing the possibilities of medical scheme benefits misuse. It can also prevent the healthcare providers from submitting false claims. This streamlines and enhances simplicity in medical scheme management.

Biometric systems can contribute to improving the quality of care and safety by linking patients to their electronic medical records. This reduces medical errors which in some cases have been fatal due to incorrect or incomplete patient records. (Department of Medical Assistance Services, 2010).

The use of biometric systems has effects on the cost of service delivery. With efficient system, the productivity of staff members in increased, translating to reduced number of staff members used to render services. Streamlined medical benefits management through the use of biometrics means money is not lost to fraud. This contributes to the reduction of service delivery cost. Unreliable biometric system on the other hand means frequent servicing and supporting the system, thus increasing system support cost. The costs could also be increased in cases where consultations with third party on medical benefits have to done through other means like telephone calls.

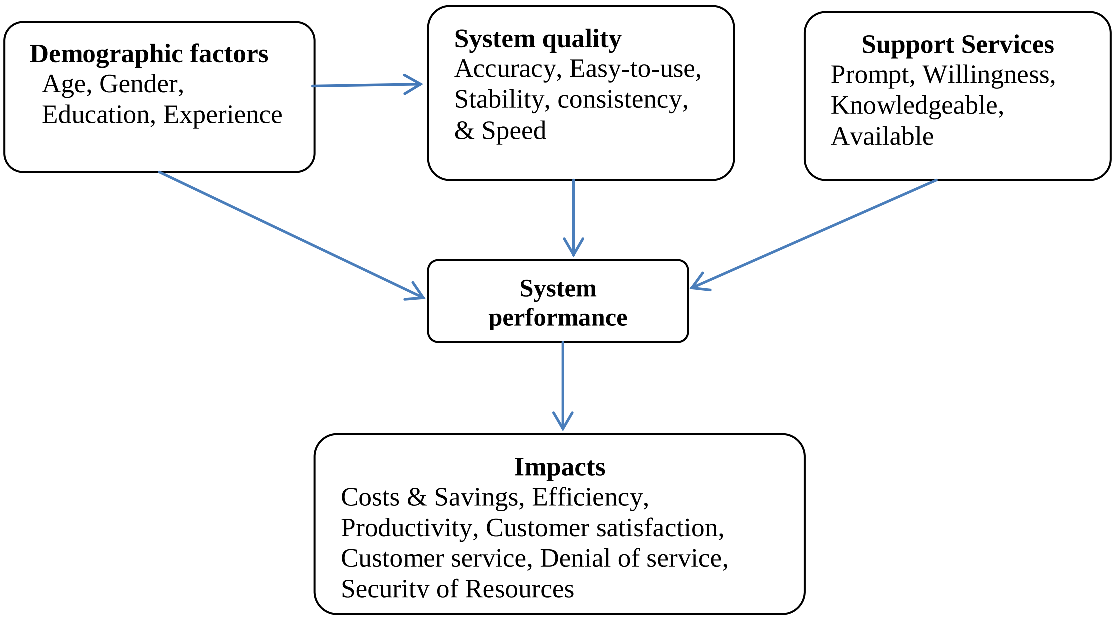
2.6 Conceptual Framework and Knowledge Gap

There are a number of reasons for the use of biometric authentication systems in healthcare. These range from error rates reduction and accuracy improvement, fraud and costs reduction, increasing safety and security, improving convenience, and conforming to legislation requirements. While the use of biometric systems has registered success, in some cases the impact has been contrary to the initial expectations (Martin, 2007).

The impact of a biometric authentication system is dependent on the performance of the system and characteristics of the users. Pato and Millett, (2011) points out a number of factors that contributes to the performance of the system which include system error rates, robustness, usability, user acceptance and security. Users are key component in the performance of biometric system as their characteristics experience level and abilities have substantial impact on the system's success. Age, gender, experience and ability can affect user's performance and influence the ability the system (NIST, 2008). System quality and IT support service quality have been identified as contributing factors to the success and impact of IT systems to individuals and organizations (DeLone and McLean 2003).

This study has adopted a conceptual model based on the above discussion as illustrated in figure 2. The framework is greatly influenced by the principles of M&L (2003) success model. M&L model provides a framework for identifying and gauging effects of variables to the system success. The conceptual framework for this study links the system performance, support services and demographic factors to the performance and impact of biometric system in service delivery. User demographic factors and the quality of IT support services offered to the users contribute to the way users perceive the qualities of the biometric system and how they use the system. The quality of system performance in terms of accuracy, stability, speed and ease of use further determine the way it is used. The willingness and manner in which the system is used determines impact on service delivery.

Figure 2.2: Conceptual Model



Source: Author 2012

Although several studies have been carried out in the field of biometric and a number on the HISs, literature review indicates that none has adequately addressed impact of biometrics systems on service delivery in healthcare. Owiti (2010) concentrated on factors affecting customer acceptance of mobile phone technology in delivery of healthcare services, which is a different technology. Abanti (2010) carried out a survey on the acceptability of biometric-based authentication system. Though his discussion and recommendation touched on the impact of biometrics system on existing hardware, he was more focused on the modalities acceptability and was limited to one private university in Kenya. Wirtz and Hercleous (2006), on a related study noted the potential of biometrics systems in improving service delivery efficiency. The findings of this study was however not conclusive according to the scholars and they recommended further investigation to enhance the validity of their findings. This study was limited in methodology as they relied on interviews with the executives who did not have first-hand interaction with the system and focused on airline sectors who's clients and operations differ with those in healthcare.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Research design

A descriptive survey involving healthcare providers in Kenya was carried out. Descriptive survey is suited in studies whose objective is to determine and describe different variables in a situation (McNabb, 2001). The descriptive survey was thus applicable in this study as the objectives were to establish the performance variables and describe how biometric authentication systems are impacting on service delivery in healthcare facilities in Kenya.

3.2 Population

The population for this study constituted of healthcare facilities in Kenya. The healthcare facilities for the purpose of this study included hospitals, clinical centres, private practitioners, laboratories and pharmacies. The internal system user formed the population for the study. The experience of the internal IT system customers was considered important for an objective assessment of the biometric system (Ribière et al., 1999). This included staff in healthcare facilities who served patients using the biometric authentication systems.

3.3 Sample design

A sample of 60 healthcare facilities in Nairobi were selected for the survey. Nairobi was considered sufficient representation of the study population, as this was where most of healthcare facilities using biometrics were found. There were 84 healthcare facilities in Nairobi (See Appendix III) out of the total 206 countrywide using biometrics. This list was drawn from AAR, UAP, AON Minet and Jubilee as preliminary investigation in 5 hospitals in Nairobi indicated that the patients using biometric cards were covered by these medical insurances companies. Random sampling was used to select a sample size of 60 healthcare facilities out of the 84 healthcare facilities that were using biometrics in Nairobi. Random sampling was chosen as it gave all the potential respondents an equal chance of inclusion in the study sample. The sample size of 60 was chosen as it was above the minimum 50 recommended where factor analysis is used to analyse data (Winter, Dodou and Wieringa, 2009). Purposive sampling was used to select respondent staff from each of the 60 healthcare facilities. The respondents included the staff who used the biometric systems to serve patients. Purpose sampling was considered suitable because not all healthcare staff used the biometric systems.

3.4 Data collection

Primary data was collected using questionnaires. The questionnaires were administered through ‘drop and pick later’. This method of distribution was chosen as direct contact with potential respondents was believed to motivate the respondents to complete the questionnaires. There were follow-up through email, phone calls and visits to ensure high response rate and to assist in cases where respondents needed clarifications.

The questionnaires consisted of both closed and open-ended questions and had three sections. The first section (A) collected the demographic data of the respondent. The second section (B) collected data regarding the performance of biometric system as viewed by the respondent. Data on factors that affect the performance of biometric systems and that had direct impact on service delivery was collected under this section. The third section (C) gathered data on the perception of the respondent on how the biometric authentication impacted on service delivery. Section B and C used Likert’s 5-point rating scale so as to allow respondents to express both the negative and positive opinion about the biometric systems.

3.5 Data Analysis

Data from the filled-in questionnaires were be coded and keyed into a computer statistics package. Statistical Package for the Social Sciences (SPSS) was used as a tool to aid in data analysis and presentation of the results.

Data collected under section A was analysed using percentage and frequency distribution to give the overall picture of the respondent and the healthcare facility. The results were presented in tables and charts. Data collected under section B was analysed with the aid of descriptive statistics of mean and standard deviation and frequency distribution. Data collected under section C was be subjected to descriptive statistic as well and factor analysis in order to determine the key impact of biometric authentication systems.

CHAPTER FOUR

DATA ANALYSIS, RESULTS AND DISCUSSION

4.1 Introduction

The return rate of the study questionnaire was good. Out of the 60 questionnaires administered, 43 were returned, resulting in a response rate of 72%, which is considered adequate for the purposes of the study. All the 43 questionnaires were duly completed and the analysis is based on data collected through these questionnaires.

4.2 Demographic Data

The study considered gender, age, education level and working experience as demographic factors that can influence the impact of biometric systems (NIST, 2008).

4.2.1 Distribution of Respondents by Gender

Majority of the respondents (67%) were male while 33% were females as presented in Table 4.1.

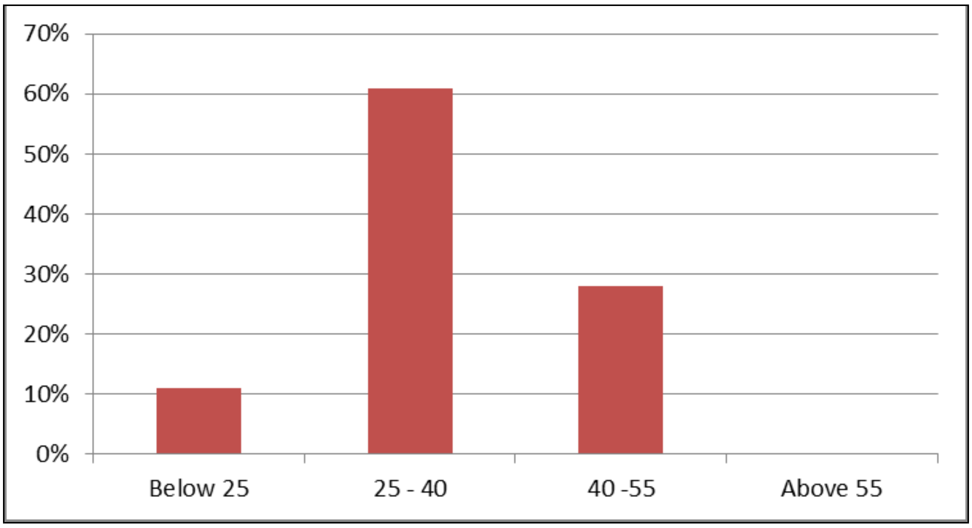
Table 4.1: Distribution of Respondents by Gender

Gender	**Frequency**	**Percentage (%)**
Male	29	67
Female	14	33
Total	**43**	**100**

4.2.2 Distribution of Respondents by Age

Majority of the respondents (60%) were in the 25 – 40 age bracket, followed by those between 40 and 55 years (28%). Those below the age of 25 years were 12%, while no respondent was above 55 years. Figure 4.1 shows the respondents distribution by age.

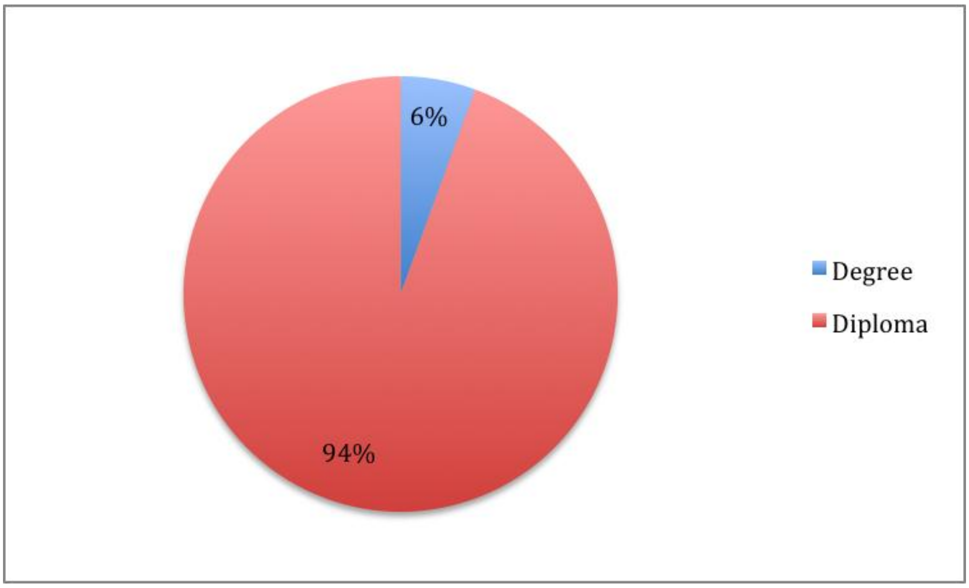
Figure 4.1: Distribution of Respondents by Age



4.2.3 Distribution of Respondents by Level of Education

The largest percentage (94%) of the respondents had attained the diploma level of education, with the rest (4%) having attained a degree level, as shown in figure 4.2 below.

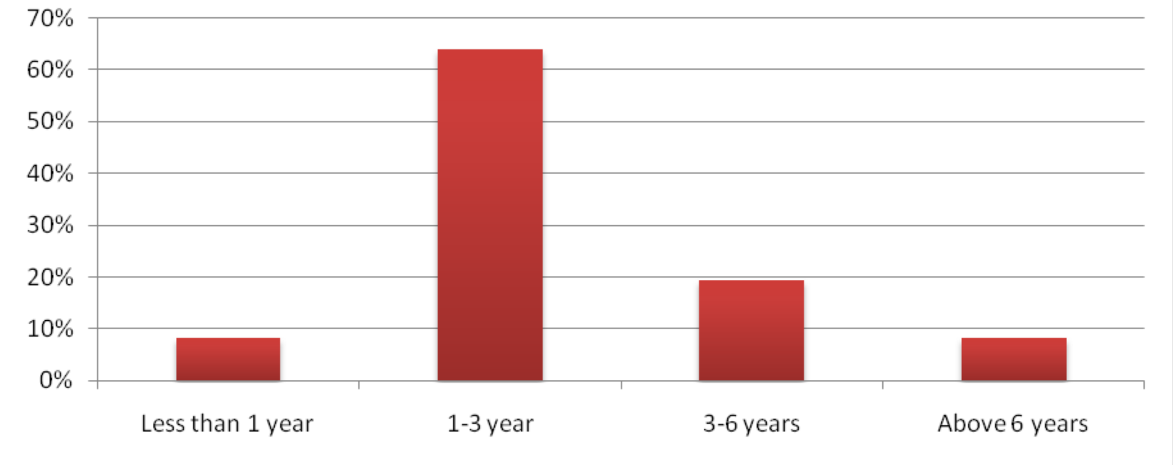
Figure 4.2: Distribution of Respondents by Level of Education



4.2.4 Distribution of Respondents by Biometric Systems Experience

Most of the respondents (64%) had working experience in biometrics of between 1 and 3 years, 19% had experience of between 3 and 6 years. A small percentage of 8% and 6% had working experience of below 1 year and over six years respectively. Thus majority of the respondents had adequate working experience of the systems to master the behaviour of the system.

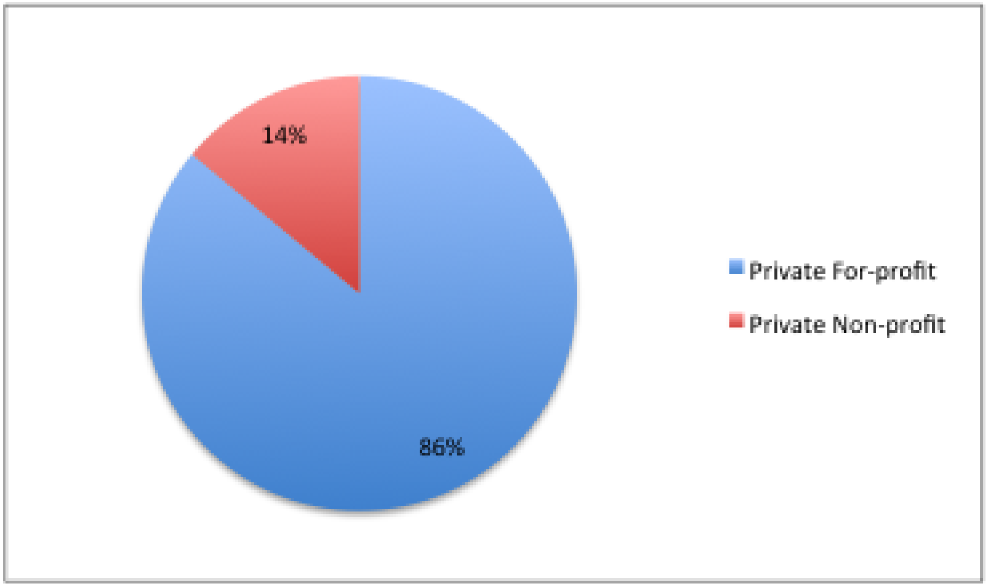
Figure 4.3: Distribution of Respondnets by Years of Working with Biometric (%)



4.2.5 Distribution of Healthcare Facilities by Type

The largest percentage (86%) of the healthcare facilities using biometrics were in the category of private for profit healthcare facilities as presented in figure 4.4. The private for non-profit took 14% .

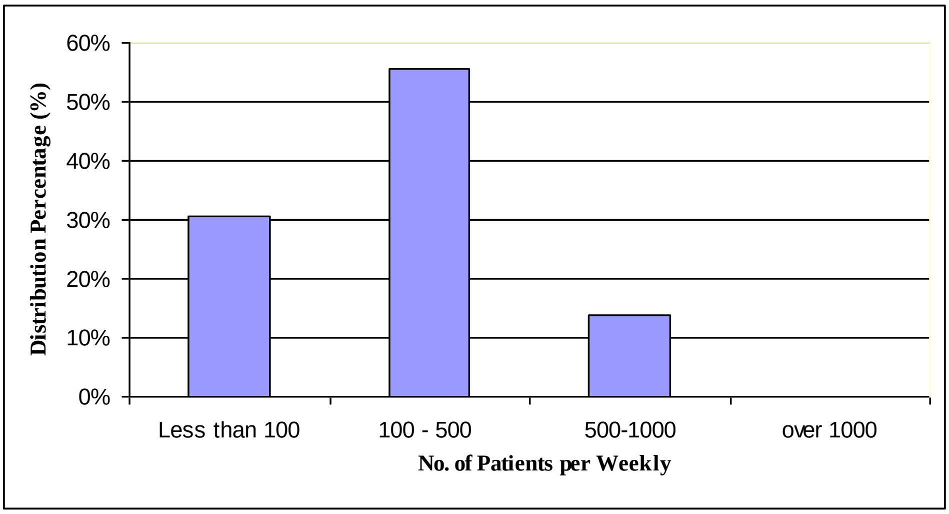
Figure 4.4: Distribution of Healthcare Facilities by Type



4.2.6 Number of Patients Served Using Biometric Systems

Most of the facilities surveyed (66%) attend to between 100 and 500 patients using biometrics on a weekly basis. Thirty per cent of the facilities were serving below 100 patients while 14% served between 500 and 1000 patients. There was no facility serving over 1000 patients per week as presented in figure 4.5.

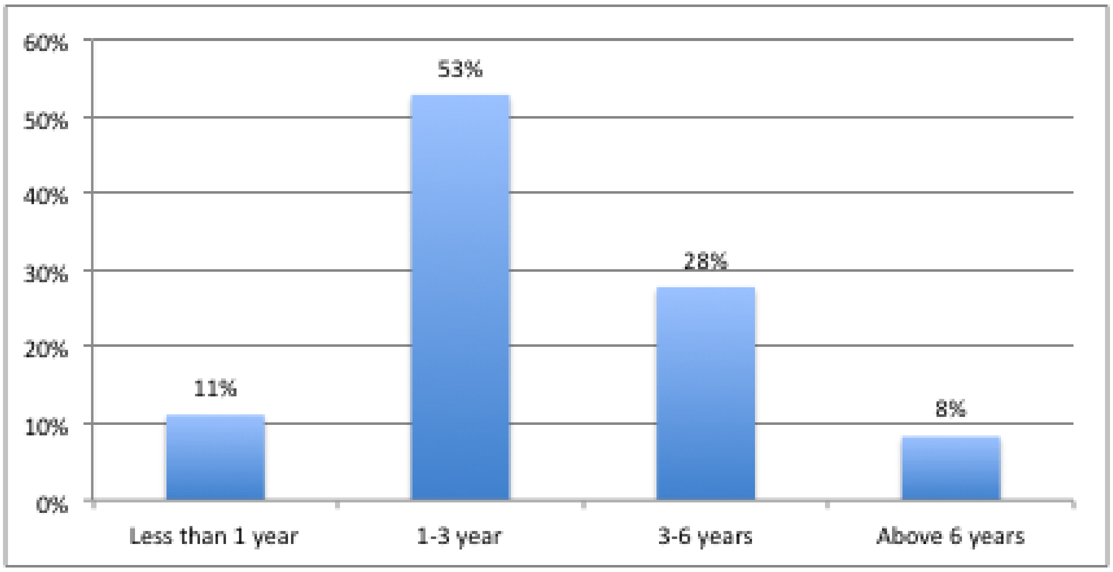
Figure 4.5: Number of Patients Served Using biometrics per Week



4.2.7 Period of Biometric System Usage in Healthcare facilities

The majority of healthcare facilities (53%) had been using biometric system for a period of 1-3 years as represented in figure 4.6. It is expected by the second and third year that the systems would be operating in a stable environment as all post implementation issues should be dealt with by then.

Figure 4.6: Distribution of Healthcare by Years of Biometrics Use



4.2.8 Types of Biometrics Use in Facilities

Ninety four per cent of the healthcare facilities used biometrics to authenticate or verify patients with a small percentage of 6% who used biometrics for patient's records access as indicated in Table 4.2.

Table 4.2: Types of Biometric Systems Use in Health Facilities

Type of Use	Frequency	Percentage
Patients Authentication	40	93%
Access of Patient's Records	3	7%
Building Access	0	0%
Others	0	0%
Total	**43**	**100%**

4.2.9 System User Training

All respondents have basic training in the use of computers and they underwent user training on how to use the biometric systems.

4.3 Factors Affecting the Performance of Biometric Authentication Systems in Healthcare Facilities

4.3.1 Effect of System Technical Qualities

All the respondents surveyed indicated that the healthcare facilities were using fingerprints as the only modality of biometric systems. There was no alternative modality meaning that in cases where the fingerprints fail, manual method of verification had to be used.

The data collected with the objective of establishing the factors affecting the performance of biometric systems was subjected to descriptive statistics of mean and standard deviation. Table 4.3 shows the ranking of these variables. The ranking is based on the Likert's five scale rating, where respondents indicated their agreement or disagreement with statements assessing the performance of system performance. The scale ratings used were, Strongly Disagree (1), Disagree (2), Neutral (3), Agree (4) and Strongly Agree (5).

The findings show that technical accuracy of the system was identified as the main weakness of the system with the ability of the system to successfully authenticate all the patients scoring a mean of 1.89 and standard deviation of 0.78 and the reliability of the biometric sensor device having a mean of 2.75 and standard deviation of 0.87.

The respondents disagreed with the statement that some patients had managed to successfully get authenticated yet not beneficiary of the claimed medical scheme with a mean of 2.08 and standard deviation of 0.65. This means that the systems are offered the intended security.

The systems user interface ease to navigate with a mean of 4.11 and standard deviation of 0.67, followed by speed in reading smartcards (4.08 mean, 0.77 standard deviation), ease in operating the system (4.06 mean, 0.75 standard deviation), and convenience to use by patients (3.97 mean, 0.65 standard deviation) were identified as qualities of biometric system that contributed to good performance of the system.

The systems' compatibility with the existing system and the system information output were ranked slightly above the neutral point, both with mean of 3.56 and standard deviation of 0.88 and 0.73 respectively. Majority of the respondents remained neutral on whether the system accepted most patients with less than 1% rejection with mean of 3.06 and standard deviation of 0.92. They were also neutral on system consistency in authenticating patients as well as whether the performance of the system is affected by weather conditions with means of 2.83 and 3.22, and standard deviation of 0.88 and 1.17 respectively.

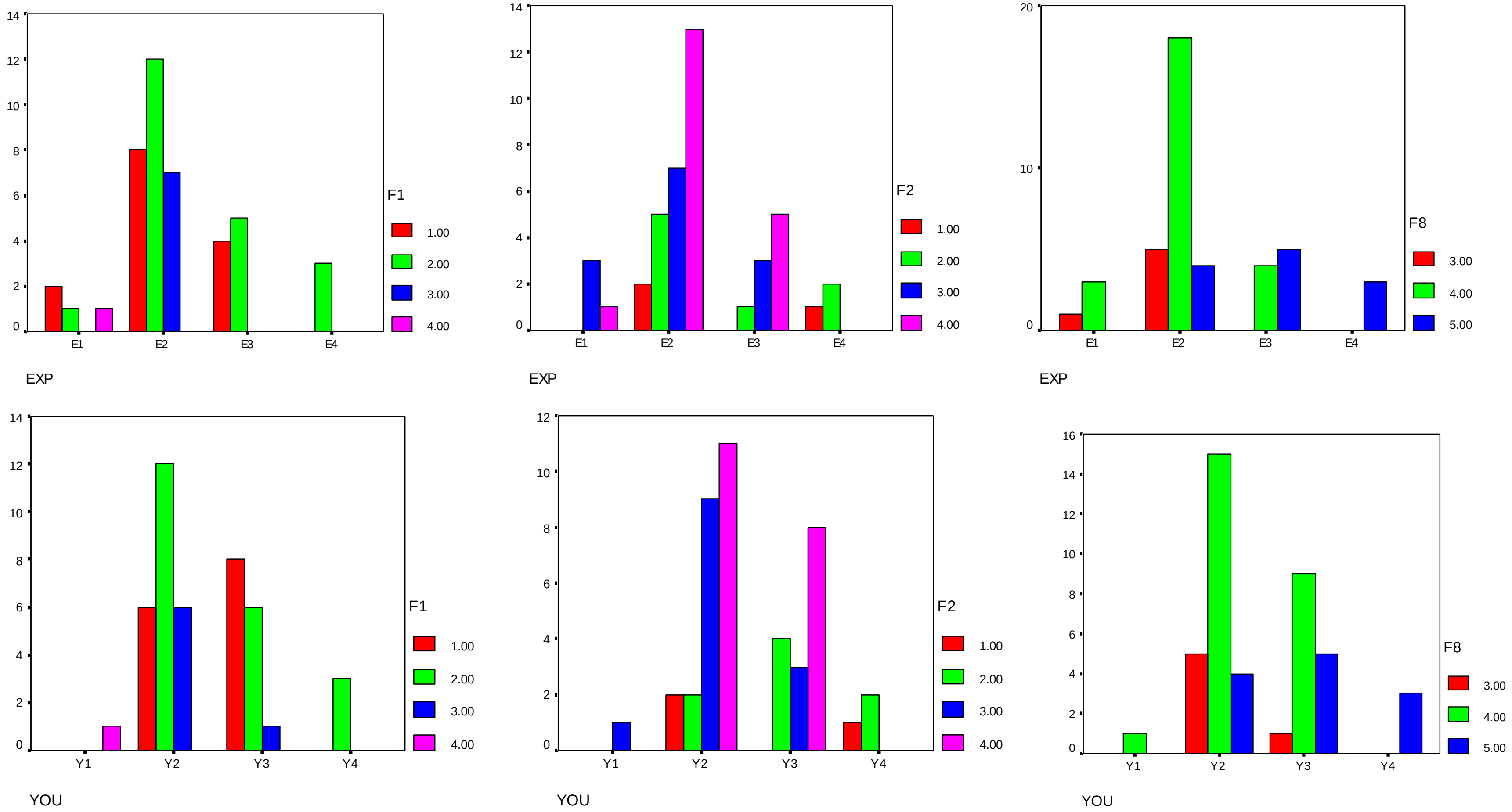
Table 4.3: Ranking of Factors Affecting the Performance of Biometric Systems

Factor	Mean	Standard Deviation
The authentication system accepts all user patients without a single rejection.	1.89	0.78
Patients trying to defraud medical scheme have been discovered through the use of biometric system.	1.92	0.51
The system has accepted patients using false documents.	2.08	0.65
Accuracy of the recognition device deteriorates with increase in number of people using it.	2.53	1.13
The recognition device needs frequent replacement.	2.58	0.81
The recognition device/sensor works reliably always	2.75	0.81
Accuracy of the recognition device deteriorates with change in weather conditions.	2.83	0.88
The authentication system accepts most user patients with less than 1% rejection.	3.06	0.92
The biometric authentication system is consistent in patient verification (results of verification don’t change from time to time for the same patient).	3.22	1.17
The information output of the system is sufficient for the intended purpose	3.56	0.73
The biometric authentication system is compatible with pre-existing information system.	3.56	0.88
Accuracy of the recognition device is affected by way the patients use the device.	3.81	0.75
The recognition device is convenience/easy to use with patients.	3.97	0.65
The system is easy to operate	4.06	0.75
The biometric system is speedy in reading the smartcards.	4.08	0.77
The system user interface is easy to navigate	4.11	0.67

4.3.2 Effects of Demographic Factors

Analysis of the demographic factors in relation to respondents perception of the factors affecting the performance of the system revealed relationship between the respondents’ years of experience and their perception on the performance of the system. Respondents who had used the system for 6 and above years had definite agreement (4 or 5) or disagreement (1 or 2) with statements presented assessing the effect of the system factors to the performance as opposed to taking neutral positions on the scale. This means the longer one used the system the better understanding of the system they had. Respondents from healthcare facilities where biometrics had been in use for longer period also had definite standing on effect of different performance variables. Figure 4.7 depicts the respondents’ perception of system performance factor based on demographic factors.

Figure 4.7: Effect of Demographic Factors on System Performance



A1: Below 25 years A2: 25 – 40 years A3: 40 – 55 years A4: Above55 years

E1: Experience below 1 year E2: 1-3yrs E3: 3-6 yrs E4: above 6yrs

Y1: Use of biometrics by healthcare below 1 year Y2: 1-3yrs Y3: 3-6 yrs Y4: above 6yrs

YOU: Years of use in a facility EXP: Respondent Experience of Biometric systems

4.3.3 Effect of IT Support Service

To establish the contribution of IT support service to the performance of the biometrics system the respondents were presented with a number of performance variables to rank them within a five points likert scale. Similar to the previous section the scale ranges from 1 to 5 with 1 indicating strong disagreement and 5 indicating strong agreement. As indicated in Table 4.4, the IT support services variables of knowledgeable IT support team and willingness of the support team to help were identified as having positive effect on the performance of the systems with a mean of 4.1 and 4.06 and a standard deviation of 0.6 and 0.7 respectively. Unavailability of internal IT support with a mean of 2.1 and lack of promptness (2.75, mean).of IT support to attend to system problems when they occur contributed to the poor performance of the system.

Table 4.4: Rankings of Support Services Factors

	Mean	Standard Deviation
Knowledgeable IT support team	4.10	0.6325
IT support willingness to help	4.06	0.7767
Availability of the IT support when required	3.47	0.7741
Prompt of IT support to solve problems	2.75	0.7319
Availability of internal IT support	2.12	0.8742

4.5 The Impact of Biometric Authentication in Service Delivery

Data collected to determine the impact of biometrics on service delivery was subjected to descriptive statistics. Findings presented in Table 4.6 show that ease to track medical benefits usage and reduction of financial loss through fraudulent claims were the main positive impact of the systems with mean of 4.06 and 4.01, and standard deviation of 0.63 and 0.62 respectively. Accuracy of verification compared to the manual method and improved speed of patients' authentication was also ranked as positive impact with high means above the neutral point of 3.91 and 3.90, and a standard deviation of 0.66 and 1.69 respectively. Further, the findings reveal that biometric systems contributed negatively to service delivery by denying patients services (2.81 mean) and failing in customer satisfaction (2.83 mean).

The respondents strongly disagreed that the system has done away with paper-based claims (1.33 mean), facilitated faster claim processing (1.44 mean), that one could serve more patients using the biometrics than those using the manual ways (1.92

mean) and that biometrics had led to reduction of staff at the service registration desk (2.47 mean).

The respondents felt that biometric authentication did not alter the quality of service delivery (3.22 mean), the speed of serving patients (3.19 mean), neither did it contribute to making it easier to do work (3.14).

Table 4.5: Impact of Biometric Systems Ranked by Mean and Standard Deviation

Variables	**Mean**	**Standard Deviation**
Biometrics system has made it easy to track medical benefits usage.	4.06	0.63
The biometric system has greatly reduced financial losses due to dishonoured fraudulent medical claims.	4.01	0.62
Biometric authentication /verification is more accurate compared to manual methods.	3.91	0.66
Biometric authentication has improved the speed of patient verification.	3.90	1.69
The patients are always willing to use system	3.50	0.77
The biometric authentication is a hindrance delivery of good service.	3.36	0.8
Biometrics authentication should be applied to all patients being served by the health facility.	3.22	1.02
The use of biometrics has improved the quality of my service delivery	3.22	0.76
Patients are always happy with service rendered using the system.	3.22	0.72
Biometrics has improved the speed of serving patients.	3.19	0.91
Biometrics authentication system makes it easier to do my work.	3.14	0.93
The use of biometric system has eliminated the use of password by patients when identify themselves using smartcards.	3.11	0.82
Patients fear the device sensor may harmful to their health.	3.01	0.61
The use of the systems has improved customer satisfaction	2.83	0.77
Some patients are unhappy with the system because of being denied services.	2.81	0.66
The use of biometrics has led to reduction of the number of staff serving at the registration desk	2.47	0.61
Some patients opt to use the paper-based system.	2.44	0.59
I can serve more patients who are using the biometric smartcards that those using manual means	1.92	0.91
Biometric systems have facilitated faster claim processing.	1.44	0.56
Biometric authentication has done away with paper-based claims.	1.33	0.48

Factor analysis aimed at reducing and grouping variables into fewer dimensions was carried out. Variables were various statements that sought to gather respondents' perception on the impact of biometrics as listed in Table 4.5, while the factors were the underlying constructs.

Principal component analysis with a varimax rotation of the 20 Likert scale questions on the impact of biometrics was conducted on data gathered from the 43 respondents. Kaiser-Meyer Olkin (KMO) test was performed on the data to measure the sampling adequacy and yielded to a KMO value of 0.498, which can be rounded off to 0.5 thus making the sample suited for factor analysis.

Table 4.6 shows 7 factors extracted using principle component analysis along with their Eigen values and the percentage of variance attributed to each factor. The 7 were the only ones with Eigen values of greater than 1 hence considered significant for analysis. The seven factors accounted for the total variance of all factors up to 78.59% as shown on the table 4.6. Each of the seven factors from one to seven accounted for 19.48%, 16.25%, 11.84%, 10.57%, 8.00%, 6.58% and 5.87% respectively.

Table 4.6: Components Extracted through Principle Component Analysis

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.90	19.49	19.49	3.90	19.49	19.49	3.09	15.44	15.44
2	3.25	16.25	35.74	3.25	16.25	35.74	2.73	13.64	29.08
3	2.37	11.84	47.58	2.37	11.84	47.58	2.70	13.50	42.57
4	2.11	10.57	58.15	2.11	10.57	58.15	2.23	11.15	53.72
5	1.60	8.00	66.15	1.60	8.00	66.15	1.72	8.59	62.31
6	1.32	6.58	72.72	1.32	6.58	72.72	1.66	8.28	70.59
7	1.17	5.87	78.59	1.17	5.87	78.59	1.60	8.00	78.59
8	0.96	4.79	83.38						
9	0.73	3.64	87.03						
10	0.53	2.62	89.65						
11	0.46	2.31	91.96						
12	0.39	1.97	93.93						
13	0.35	1.77	95.69						
14	0.31	1.56	97.25						
15	0.25	1.24	98.49						
16	0.14	0.68	99.17						
17	0.10	0.48	99.65						
18	0.04	0.20	99.85						
19	0.02	0.12	99.97						
20	0.01	0.03	100.00						
Extraction Method: Principal Component Analysis.									

Table 4.7: Rotated Component Matrix

	Component						
	1	**2**	**3**	**4**	**5**	**6**	**7**
F1	0.4	0.4	0.7	0.0	-0.2	-0.2	0.2
F2	0.2	0.7	-0.4	-0.1	0.3	0.1	0.0
F3	-0.1	0.8	0.4	-0.4	-0.1	-0.2	0.1
F4	0.3	-0.4	0.0	0.6	0.3	0.1	-0.3
F5	0.4	0.0	0.6	0.1	0.1	0.0	-0.4
F6	0.1	0.9	0.1	-0.1	0.0	-0.2	0.0
F7	-0.1	0.8	0.2	0.1	-0.1	0.1	0.0
F8	0.7	0.2	0.6	-0.2	0.0	-0.2	0.1
F9	-0.1	0.2	0.1	0.8	0.1	0.0	0.1
F10	0.0	-0.1	0.2	0.1	0.7	0.1	-0.7
F11	0.0	0.1	-0.2	-0.1	0.8	0.2	-0.1
F12	-0.2	-0.1	0.0	0.0	0.2	-0.1	0.7
F13	-0.4	0.1	0.4	-0.6	0.1	-0.1	0.0
F14	0.0	-0.2	0.0	0.7	-0.2	0.2	0.2
F15	0.0	-0.2	0.9	0.2	0.1	0.1	0.0
F16	0.9	0.0	0.0	0.1	0.1	0.0	0.1
F17	0.9	0.0	-0.1	0.0	0.0	0.0	0.1
F18	0.1	-0.2	0.0	0.1	-0.3	0.8	0.0
F19	0.2	0.1	-0.2	-0.1	0.4	0.1	-0.1
F20	-0.2	0.2	-0.1	0.1	0.2	0.8	0.2
Extraction Method: Principal Component Analysis.							
Rotation Method: Varimax with Kaiser Normalization.							

Table 4.7 shows loading of each variable on the seven factors and table 4.8 shows the variables constituting each of the factors. The minimum loading considered for each factor was 0.5.

Table 4.8: Variable Loading on Factors

Factor	Variables
Factor 1	• Biometric system has eliminated the use of password with smartcards by patients. • Patients are always willing to use system. • Biometric system has greatly reduced financial losses to the organization due to dishonored fraudulent medical claims.
Factor 2	• Biometric authentication has improved the speed of patient verification. • Biometrics has improved the speed of serving patients. • I can serve more patients who are using the biometric smartcards that those using manual means • Biometric authentication/verification is more accurate compared to manual methods.
Factor 3	• Biometric authentication has done away with paper-based claims. • Use of biometrics has improved the quality of my service delivery. • Biometric systems have facilitated faster medical claims processing.
Factor 4	• Biometrics authentication system makes it easier to do my work • Patients are happy with services rendered using biometric system • Biometric system has made it easy to track patient's medical benefits usage
Factor 5	• Use of biometric systems has improved customer satisfaction • I am happy to serve patients using the biometric system
Factor 6	• Some patients opt to use the paper-based system • some patients are unhappy with the system because of being denied services
Factor 7	• Biometric authentication is a hindrance to good service delivery

Factor 1 loaded highly on the use of biometric system has eliminated the use of password with smartcards by patients, the patients are always willing to use system and biometric system has greatly reduced financial losses to the organization due to dishonored fraudulent medical claims. These variables relates mostly to the security offered biometric systems.

Factor 2 loaded on four variables which relates to the efficiency in service delivery. The variables were biometric authentication has improved the speed of patient verification, biometrics has improved the speed of serving patients, respondents could serve more patients who are using the biometric smartcards that those using manual means and biometric authentication/verification is more accurate compared to manual methods.

Factor 3 loaded onto variables associated with costs and savings brought by IT automation of process. The variables were biometric authentication has done away with paper-based claims, the use of biometrics has improved the quality of my service delivery and biometric systems have facilitated faster medical claims processing.

Three variables loaded on Factor 4, biometrics authentication system makes it easier to do my work, patients are happy with services rendered using biometric system and biometric system has made it easy to track patient's medical benefits usage. These variables relate to convenience of biometrics.

Two variables loaded on to Factor 5, the use of biometric systems has improved customer satisfaction and respondents were happy to serve patients using the biometric system. These relates to satisfaction with the biometric system by both internal and external users.

Factor 6 consists of 2 variables, some patients opt to use the paper-based system and some patients are unhappy with the system because of being denied services. These can be labelled as service denial.

Factor 7 loaded only to one variable, biometric authentication is a hindrance to good service delivery.

The key impact can be summarized under security, efficiency in service delivery, cost and savings, convenience, customer satisfaction, service denial and hindrance to excellent service delivery headings.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter presents summaries from the data analysis, draws conclusion and gives recommendations.

5.2 Summary

The research established that the majority users (86%) of biometric systems are private for profit healthcare facilities. Biometrics has been in use in a small number (8%) of healthcare facilities for over six years, and the majority (53%) of the surveyed facilities had embraced the technology between 1and 3 years ago. The survey found that the biometric system modality used in all healthcare facilities surveyed was fingerprints and biometrics was mainly (93%) used to verify users with a small percentage using it to access medical records.

The study established user demographics, system quality and services offered by IT support had impacted on the performance of biometric systems used in healthcare facilities. This was in line with what literature review had premised. The performance factors were categorized into two groups, inhibitors and enablers of good performance as presented in Table 5.1.

Table 5.1: Factors Affecting the Performance of Biometric systems

Enabling Factors	**Inhibiting Factors**
Response time Ease to operate Sufficient information output Security Knowledgeable IT support IT support willingness to help Ability to withstand large number of users Ease of use with patients User experience	Technical Accuracy Reliability Patients manner of usage Promptness of IT support

The majority of the respondents identified system response time, ease in operating the system, adequacy of system output, knowledgeable and willingness of the IT support as enabling factors to good performance of biometric system.

System technical accuracy was identified as a major inhibiting factor to the performance of the systems as the systems could not positively verify all the patients qualifying for service. Other inhibiting factors included the recognition sensor reliability, the patients' manner of use and the promptness of the IT support. Analysis of demographic factors indicated that experience in the use of the system affected the way the respondents viewed the performance of the system.

The findings from data collected in pursuant to objective 2 of the study, show that biometric system had made it easier for the health facilities to track the medical benefits, offered security as it had deterred medical fraudsters, made it quick to verify patients and reduced financial loss through medical scheme fraud.

Although the respondents indicated that verifying of patients using biometrics was faster than the manual way, the findings indicate that biometrics had no impact on the efficiency in service delivery as they disagreement that biometrics had not done away with manual claim processes, improved the speed of servicing a patient and facilitated faster claim processing.

Further, the findings revealed that the systems had not contributed to betterment of service delivery. Most of the respondents were neutral to whether biometrics had improved their service delivery quality or made their work easier. They also disagreed that biometrics had improved customer satisfaction.

5.3 Conclusion

The study achieved the study objectives and answered the research question. The findings of this study established a number of factors affecting the performance of biometric systems in healthcare facilities in Kenya as listed in Table 5.1. The study further demonstrated that use of the biometric systems in healthcare facilities had positively and negatively impacted on service delivery.

Contrary to expectations of literature review, the study found out that use of biometrics did not result to efficiency or improved customer service. Although biometrics systems have achieved the security intend, a different solution may be necessary for overall positive impact on service delivery.

5.4 Limitations of the study

Time was the main constraining factor during this study and as such the scope of this study was limited to Nairobi only. A number of respondents were unable to complete the administered questionnaires and owing to the inadequate time it was not possible to get the more respondents to attain the targeted sample size for the study, and completed the study on time.

Availability of literature especially local literature on the subject of biometrics was another major limitation to the study. There was very little publication on local content.

5.5 Recommendations

This study found out that the entire healthcare facilitates survey used fingerprints modality for patients' authentication. Although biometric systems had been in operation for over 6 years, there was need for an improved solution in order to reap the maximum benefits of these systems. It was also established that system errors and specifically false rejection error was the main factor adversary affecting the performance of biometric system. As such the healthcare facilities may wish to deployment of a multi-biometrics solution. This will ensure that the patients are not denied services due to inadequacies of the unibiometric system.

5.5.1 Recommendation for Further Research

This study focused on the healthcare facilities' internal users of biometric system. Healthcare facilities being a service industry, the perception of external users is a necessary contribution when assessing the performance and the impact of the biometric systems. Therefore a study to find out the patients perception of the system is recommended.

REFERENCES

Abanti, C. (2010) Acceptability Survey of Biometric-Based Authentication System. *Anthology of Abstracts of the 3rd International Conference on ICT for Africa, M*arch 25-27, Yaoundé, Cameroon. Baton Rouge, LA: International Center for IT and Development.

Anil K. Jain, Arun A. Ross and Karthik Nandakumar (2011) *Introduction to Biometrics,* Pages 259-306

APHIA (2001). *The Kenya Hospital Management Information System*. APHIA Financing and Sustainability Project (Contract Number 623-0264-C-00-7005-00).

Baily, C. A. (1996). *A Guide to Field Research*. Thousand Oaks, CA: Pine Forge Press.

Barnes, J., Hanlon, B., Feeley III, F., McKeon, K., Gitonga, N. and Decker, C. (2010). *Private Health Sector Assessment in Kenya*. World Bank working Paper No.193

Biometrics in Healthcare. (2009). In findBiometrics. Retrieved June 30, 2012, from http://www.findbiometrics.com/health-care/

Chandra, A., & Calderon, T. (2005). Challenges and constraints to the diffusion of biometrics in information systems. *Communications of the ACM*, 48(12), 101- 106.

Coats, W. S., Bagdasarian, A., Helou, T. J. and Lam, T. (2007). The practitioner's guide to biometrics. ABA Publishing, Chicago.

DeCoster, J. (1998). *Overview of Factor Analysis*. Retrieved August 04, 2012 from http://www.stat-help.com/notes.html

Emre, A. (2000). Biometric Security Technologies. Retrieved June 27, 2012, from "http://ai.pku.edu.cn/aiwebsite/research.files/collected%20papers%20-%20introduction/biometric%20security%20technologies.pdf"

European Community. (2005). *Biometrics at the Frontiers: Assessing the impact on Society*. Technical Report Series (EUR 21585 EN).

Grijpink, J.H.A.M., (2004). Two barriers to realizing the benefits of biometrics: A chain perspective on biometrics, and identity fraud as biometrics' real challenge, in: Optical Security and Counterfeit Deterrence Techniques V, edited by Rudolf L. van Renesse, Proceedings of SPIE-IS&T Electronic Imaging, SPIE Vol. 5310, pp. 90-102

Healthcare IT News (2005). Biometrics Bring Fingerprint ID to Hospitals. Retrieved July 11, 2012, from http://www.eweek.com/c/a/Health-Care-IT/Biometrics-Bring-Fingerprint-ID-to-Hospitals/

Heracleous, L., and Wirtz, J. (2006). Biometrics: the Next Frontier in Service excellence, Productivity and Security in the Service Sector. *Managing Service Quality*, 16 (1) 12-22 DOI: 10.1108/09604520610639937

Homeland Security News Wire, (2011, June 10). *Malaysia's Biometric Failure*. Retrieved June 5, 2012 from http://www.homelandsecuritynewswire.com/malaysias-biometric-failure.

iHealthBeat. (August 01, 2002). *Alabama health system installs biometric ID system to manage access to patient records.* Retrieved June 5, 2012 from http://www.ihealthbeat.org/articles/2002/8/1/

Iselin, N. J. (February 28, 2011). *OTI Expands Medismart with Orders for an Additional 100,000 Cards In Kenya.* Retrieved May 29, 2012 from “http://www.otiglobal.com/OTI_Expands_MediSmart_with_Orders_for_Additional_Cards_in_Kenya”

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

Jain, A., Hong, L., and Pankanti, S. (2000). Biometric Identification. *Communications of the ACM*, 43(2) 91-98

Kenyan Insight (July 31, 2012). Kajwang’ tells IEBC to forget Biometric Voter Registration. Retrieved from August 13, 2012 from http://www.kenyaninsight.com/kajwang-tells-iebc-to-forget-biometric-voter-registration/

M2SYS (2010). *The largest hospitals in Angola to Use Fingerprint Biometrics for Patient Identification*. Retrieved on June 10, 2012 from http://www.m2sys.com/pr012510.htm

Marco Gamassi, Massimo Lazzaroni, Mauro Misino, Vincenzo Piuri, Daniele Sana, and Fabio Scotti. (2004). Accuracy and Performance of Biometric Systems. Technology Conference Como, Italy, 18-20 May 2004

Martin, Z. (2007). A New Application for Biometrics. *Health Data Management Magazine*. http://www.healthdatamanagement.com/issues/2007_42/25273-1.html

Mbogo, S. (2011, January 31). Health insurers tap bio-card to stem surging fraud cases. *Business Daily*. Retrieved from http://www.businessdailyafrica.com/Corporate+News/Health+insurers+tap+bio+card+to+stem+surging+fraud+cases/-/539550/1098672/-/item/2/-/1dvjo6z/-/index.html

Ministry of Health & Ministry of Public Health. (2009). *Health Sector Strategic Plan for Health Information System 2009-2014.* Retrieved July 9, 2012, from http://www.medical.go.ke/index.php?option=com_content&view=article&id=68:downloa.

Ministry of Public Health and Sanitation and the Ministry of Medical services (2012). *eHealth-Kenya Facilities.* Retrieve July 15, 2012, from http://www.ehealth.or.ke/facilities/default.aspx

Muga, R., Kizito, P., Mbayah, M., & Terry Gakuruh, T. (2004). *Demographic and Health Surveys: Overview of the Health*. Retrieved June 29, 2012, from www.measuredhs.com/pubs/pdf/spa8/02chapter2.pdf

National Coordinating Agency for Population and Development (NCAPD) [Kenya], Ministry of Health (MOH), Central Bureau of Statistics (CBS), ORC Macro. (2005). *Kenya Service Provision Assessment Survey 2004*. Nairobi, Kenya:

Ndavi, P.M., S. Ogola, P.M. Kizito, and K. Johnson. 2009. *Decentralizing Kenya's Health Management System: An Evaluation.* Kenya Working Papers No. 1. Calverton, Maryland, USA: Macro International Inc.

Neurotechnology. (July 11, 2011). *Kenya's New Electronic Voter Registration System.* Retrieved June 13, 2012, http://www.neurotechnology.com/

Obeng, P. (2008). Assessing the impact of Technology on Banking Service Delivery and Bank/Customer relationship: A case study of SG-SSB Limited, Kumasi Main Branch (Masters Thesis). http://hdl.handle.net/123456789/1477

Omachonu, V.K. and Einspruch N.V., (2010). Innovation in Healthcare Delivery. *The Innovation Journal: The Public Sector Innovation Journal,* vol. 15(2)

Pardesi, J. D. (2007). *Emerging Trends in Information Technology*. Nirali Prakshan, India

Pato, J. N. and Millett. L. I. (Eds.)(2011). Biometric Recognition: Challenges and Opportunities.

Schneider, J.K., and Price, J.H. (2001) Positive Outcomes Implementing Biometrics in Multiple HealthCare Applications. *TEPR 2001 Conference and Exhibition*

Shoniregun, C.A., and Crosier, S.(2008). *Securing Biometrics Applications* Springer, USA.

ThirdFactor. (2011, Feb 28). *OTI ships 100,000 more MediSmart cards to Kenya*. Retrieved July 12, 2011, from "http://www.thirdfactor.com/2011/02/28/oti-ships-100-000-more-medismart-cards-to-kenya".

Winter, J. C. F., Dodou, D. and Wieringa, P. A. (2009). Exploratory Factor Analysis With Small Sample Sizes *Multivariate Behavioral Research,* 44 147–181.

Wirtz, J. and Heracleous, L. (2005). Biometrics meets services. *Harvard Business Review*, February, p. 48.

Woodward, J. D., Orlans, N. M., and Higgins, P. T. (2003). *Biometrics*. McGraw-Hill/Osborne

Zhang, D. (2000). *Automated Biometrics: Technologies and Systems.* Kluwer Academic Publishers, USA

APPENDICES

Appendix I: Introduction Letter

UNIVERSITY OF NAIROBI

SCHOOL OF BUSINESS

Telephone: +254-2-318262
Telegrams: "Varsity", Nairobi
Telex: 22095 Varsity

Martha Mulumba
PO.Box 30711- 00100
Nairobi, Kenya

Dear Sir/Madam,

RE: A SURVEY OF BIOMETRIC AUTHENTICATION SYSTEMS AND SERVICE DELIVERY IN HEALTHCARE SECTOR IN KENYA.

I am a postgraduate student at the University of Nairobi undertaking Master in Business Administration (MBA). As part of my course requirement, am carrying out a survey on Biometric Authentication Systems and Service Delivery in Healthcare Sector in Kenya.

I am hereby requesting you to assist me by completing the attached questionnaire. Please be assured the information collected through the questionnaire shall be used for the purpose of academic study only and shall be treated in confidentiality. A copy of this research project will be made available to you upon request.

Yours faithfully,
Martha Mulumba,
MBA Student, University of Nairobi.

Appendix II: Questionnaire

A SURVEY OF BIOMETRIC AUTHENTICATION SYSTEMS AND SERVICE DELIVERY IN HEALTHCARE SECTOR IN KENYA

Section A: Demographic Data

1. Select your gender. □ Male □ Female

2. What is your age?

   □ Less than 25 years □ 25 – 40 years

   □ 40 - 55 years □ 55 years and above

3. Please indicate your highest level of education.

   □ Primary □ High school □ Diploma □ Degree

4. How long have you been working with the biometric systems?

   □ Less than 1 year □ 1 – 3 years

   □ 3 - 6 years □ 6 years and above

5. How many patients using the biometric smartcards does your healthcare facility serve in a week?

   □ Less than 100 □ 100 – 500

   □ 500 – 1000 □ 1000 and above

6. In what category does your healthcare facility fall under

   □ Public

   □ Private For-profit

   □ Private Non-Profit

7. How long has your healthcare facility been using biometric systems?

   □ Less than 1 year □ 1 – 3 years

   □ 3 - 6 years □ 6 years and above

8. In which area are biometrics in use your health facility? Tick all that apply.

   □ Patient authentication/verification □ Building Access

   □ Patient's medical records access □ Others (Specify) --------------

With the introduction of biometric system, did your healthcare facility undertake training for the staff? □ Yes □No

----

Section B: System Technical Performance and Support Data

1. What type of biometric modalities is your facility using? Tick all that apply.

□ Fingerprints

□ Hand Geometry

□ Palm Vein recognition

□ Others (State): ___________________________

□ Do not know

2. To what extent do you agree or disagree with the following statements about biometric system performance

	Strongly Disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
	1	**2**	**3**	**4**	**5**
1. The authentication system accepts all user patients without a single rejection.					
2. The authentication system accepts most user patients with less than 1% rejection.					
3. Patients trying to defraud medical scheme have been discovered through the use of biometric system.					
4. The system has accepted patients using false documents.					
5. The biometric system is speedy in reading the smartcards.					
6. The biometric authentication system is consistent in patient verification (results of verification don't change from time to time for the same patient).					
7. The system user interface is easy to navigate					
8. The information output of the system is sufficient for the intended purpose					

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
	1	**2**	**3**	**4**	**5**
9. The recognition device is convenience/easy to use with patients.					
10. The recognition device/sensor works reliably always					
11. Accuracy of the recognition device deteriorates with increase in number of people using it.					
12. Accuracy of the recognition device deteriorates with change in weather conditions.					
13. Accuracy of the recognition device is affected by way the patients use the device.					
14. The recognition device needs frequent replacement.					
15. The system is easy to operate					
16. The biometric authentication system is compatible with pre-existing information system.					

3. Please indicate how you agree with the following statements about system support by the information technology (IT) support team.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
	1	**2**	**3**	**4**	**5**
1. The IT support team is usually available to solve system problems whenever they occur					
2. The IT support team responds promptly when a problem occur					
3. The IT support team is highly knowledgeable in biometric system					
4. The IT team is always willing to help					
5. The IT support team is part of healthcare employees					

Section C: Impact of Biometrics System

1. To what extent do you agreed with the following statement about the effects of biometric authentication systems

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
	1	2	3	4	5
1. Biometric authentication has done away with paper-based claims.					
2. Biometric authentication has improved the speed of patient verification.					
3. Biometrics has improved the speed of serving patients.					
4. Biometrics authentication system makes it easier to do my work.					
5. The use of biometrics has improved the quality of my service delivery.					
6. I can serve more patients who are using the biometric smartcards that those using manual means.					
7. Biometric authentication/verification is more accurate compared to manual methods.					
8. The biometric system has greatly reduced financial losses to the organization due to dishonored fraudulent medical claims.					
9. The use of biometrics has led to reduction of the number of staff serving at the registration desk					
10. Biometrics system has made it easy to track patient’s medical benefits usage.					
11. Biometric systems have facilitated faster medical claims processing.					
12. The use of biometric system has eliminated the use of password with smartcards by patients.					
13. The patients are always willing to use system.					
14. Some patients are unhappy with the system because of being denied services.					

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
	1	**2**	**3**	**4**	**5**
15. Patients fear the device sensor may harmful to their health.					
16. Some patients opt to use the paper-based system.					
17. Patients are happy with services rendered using biometric system.					
18. The use of biometric systems has improved customer satisfaction.					
19. I am happy to serve patients using the biometric system.					
20. Biometric authentication is a hindrance to good service delivery.					

Appendix III: List of Health Facilities Using Biometric in Nairobi

Healthcare Facility	Location
1. AAR Health Services	Community
2. Acacia Medical Centre	Ralph Bunche
3. Afya Royal Clinics	Ngong Road
4. Aga Khan University Hospital	Limuru Road
5. Akuhn Diagnostic Centres	Parklands
6. Alkam Laboratory Services	City Centre
7. Ankh Womens Clinic	NHIF Building
8. Avenue Hospital	Parklands
9. Baus Optical	City Centre
10. Ben Ammi Medical Centre	Community
11. Cambridge & Company Ltd	City Centre
12. Canaan Health Provider	City Centre
13. Cape Dental	Yaya
14. Chiromo Lane Medical Centre	Parklands
15. Consolidated Diagnostic Imaging Centre	City Centre
16. Coptic Hospital	Ngong Road
17. Dental Health Providers Limited	Ngong Road
18. Dentplan Dental Surgeons	City Centre
19. Edelvale Trust Jamaa Home & Hospital	Donholm
20. Eltons Pharmacy Ltd	City Centre
21. Equitorial Medical Centre	Komarok
22. Executive Dental	City Centre
23. Eye Care Consultants Ltd	City Centre
24. Eyestyle Opticians	Westlands
25. First Laser Skin Centre	Yaya
26. Garlands Medical Centre	Rongai
27. Gertrudes Children Hospital	Muthaiga
28. Gilead Medical Centre	City Centre
29. Guru Nanak Ramgarhia Sikh Hospital	Ngara
30. Hurlingham Comprehensive Healthcare Clinics(Hurlingham ENT)	Hurlingham
31. Innovative Dental Clinic	Wabera Street
32. International Medical Consultants(K) Ltd	Ralph Bunche
33. Jacaranda Chemist	City Centre
34. Jaff's Optical House Ltd	Westlands
35. Jamaa Hospital	Buruburu
36. Jamko Health Clinic & Laboratory	Argwings Kodhek
37. Kam Health Services	City Centre
38. Kam Pharmacy	City Centre
39. Karen Hospital	Karen
40. Kenyatta National Hospital(Private Wing)	Community
41. Kitengela Medical Services	Kitengela

Healthcare Facility	Location
42. Komarock Medical Centre	Komarock
43. Langata Comprehensive Medical Service	Langata
44. Langata Hospital	Langata
45. Langata Integrated Health Services	Langata
46. Lions Sightfirst Eye Hospital	Westlands
47. Lions Sightfirsteye Hospital	Loresho
48. Lunettes Opticians (Dr. Soroya)	Lavington
49. Lyntons Pharmacy Ltd	City Centre
50. M P Shah Hospital	Parklands
51. Malibu Pharmacy Ltd	City Centre
52. Mater Hospital	Industrial Area
53. Melchizedek Hospital	Ngong Road
54. Mercy Medical Centre	City Centre
55. Meridian Medical Centre Yaya Centre	Yaya
56. Metropolitan Chemist	City Centre
57. Metropolitan Hospital	Buru Buru
58. Molars Limited	City Centre
59. Nairobi Childrens Clinic	Ralph Bunche
60. Nairobi Diagnostic Laboratories	Ralph Bunche
61. Nairobi Eye Associates	Ralph Bunche
62. Nairobi Hospital	Argwings Kodhek
63. Nairobi MRI Centre	Ngong Road
64. Nairobi South Medical Centre	South C
65. Nairobi West Hospital	Nairobi West
66. Nairobi Womens Hospital	Ngong Road
67. Nature Chemist	Buru Buru
68. Njimia Wendani	Kahawa
69. Omega Opticians	City Centre
70. Optica Ltd	Westlands
71. Optimum Medical Centre	City Centre
72. Plaza MRI	Ralph Bunche
73. Plaza X Ray Services	City Centre
74. Prestige Dental Services	Argwings Kodhek
75. Prime Care Heart Clinic	Argwings Kodhek
76. Ruaraka Uhai Neema Hospital	Ruaraka
77. Savannah Healthcare	City Centre
78. Seventh Day Adventists Health Services	Milimani
79. Sinai Mount Hospital	Rongai
80. St Francis Community Hospital	Thika Road
81. Star Optics Ltd	City Centre
82. Thika Road Health Services Ltd	Ruaraka
83. Upper Hill Medical Centre	Ralph Bunche
84. Westlands Medical Centre	Westlands

Source: AAR, AON Minet brokers, Jubilee Insurance and UAP Insurance