UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

A FRAMEWORK FOR THE ADOPTION OF BIOMETRIC ATM AUTHENTICATION IN THE KENYAN FINANCIAL INSTITUTIONS

BY

ONYWOKI BENSON MAKORI

RESEARCH PROJECT REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF THE DEGREE OF MASTER OF SCIENCE IN INFORMATION SYSTEMS (MSC.IS) OF THE UNIVERSITY OF NAIROBI.

MAY 2014

DECLARATION

I, Onywoki Benson Makori, do hereby declare that this research project report is entirely my own work and where there is contribution of other individuals, it has been duly acknowledged. To the best of my knowledge, this research work has not been carried out before or previously presented in any educational institution for any award.

Signature---------- Date----------

Onywoki Benson Makori

P56/73424/2012

I, Dr Elisha T. Opiyo Omulo, do hereby certify that this project report has been presented for examination with my approval as the University of Nairobi supervisor.

Signature---------- Date----------

Dr Elisha T. Opiyo Omulo

ACKNOWLEDGEMENTS

Firstly, I would like to express my deepest gratitude to God for His blessings, strength and grace that has enabled me to complete this project. My sincere gratitude goes to my supervisor Dr. Elisha T. Opiyo Omulo for his constant guidance, positive criticism and above all his viable suggestions and priceless advice throughout my project work, which tremendously contributed to my success within the shortest time possible. I would like to thank my family for their endless support, patience and love throughout the project period. I sincerely appreciate their personal sacrifices that enabled me achieve the project goals. I will also not forget to acknowledge the contributions from individuals and organizations that made this project a success. Without their support, it would be impossible to accomplish this task.

ABSTRACT

The use of ATMs has become fundamental in the financial institutions owing to the values that are transacted using these systems and the 24/7 availability of these systems. Although several researchers have discussed the role of biometrics in security applications for financial institutions, no systematic empirical research has been applied to studying the role of organizational characteristics and contextual factors in the Kenyan financial sector. This study sought to develop a framework for the adoption of biometric ATMs in the in the Kenyan financial institutions apply the developed framework to study factors influencing adoption of biometric ATM authentication as well as validate the conceptual framework. A survey was used to collect quantitative data from the customers on the model's predictors; intention to use and individual characteristics was used. The data sample was then analysed factor analysis and multiple regression analysis. The study established that performance expectancy, effort expectancy, social influence and user privacy were key determinants for biometric ATMs acceptance, adoption and usage. The study further demonstrated that age, gender and experience were moderating factors on effort expectancy. Experience was a moderating factor on performance expectancy, effort expectancy, social influence and user privacy.

Key words: framework, adoption, authentication, financial institutions

TABLE OF CONTENTS

KEY DEFINITIONS

Biometrics - This is a science and technique for recognizing the human characters, both physiological and behavioral. (Gaur et al, 2012)

Authentication - Corcoran et al., (2000) describes authentication as the process of associating an individual with his/her' unique identity, which is the manner he/she establishes the validity of his/her claimed identity.

Model – this is a conceptual structure intended to serve as a guide for developing something that expands the structure into something useful.

Adoption – means to choose as a standard or required in a course.

Effort expectancy: The degree of ease associated with the use of the system.

Attitude: Individual's positive or negative feeling about performing the target behavior (e.g., using a system).

Behavioral intention: The degree to which a person has formulated conscious plans to perform or not perform some specified future behavior.

Performance expectancy: The degree to which an individual believes that using the system will help him or her to attain gains in job performance.

Perceived usefulness: See the definition of performance expectancy.

Subjective norm: Person's perception that most people who are important to him think he should or should not perform the behavior in question.

Dependent variable – is a variable of primary interest to the study. It is also known as criterion of the study.

Independent variable – this is a variable that influences or determines the dependent variable.

Generalizability – the probability that the results of a research apply to other groups, setting s or conditions.

Methodology – this is a plan of action or a set of methods applied to a field of study.

Pilot study – this is a study conducted to detect design weaknesses as well as fine tuning the data collection instruments.

Reliability – this is the extent to which research findings would be the same if the research was to be conducted on a later date with different samples.

Questionnaire – a research instrument consisting of a series of questions and other prompts for the purpose of gathering information from respondents.

Interview - a conversation between two or more people where questions are asked by the interviewer to elicit facts or statements from the interviewee.

Sample – this is a subject of the population, comprising some members selected from the population.

LIST OF ABBREVIATIONS

ATM	Automatic Teller Machine
TRA	Theory of Reasoned Action
TPB	Theory of Planned Behavior
IDT	Innovation Diffusion Theory.
SCT	Social Cognitive Theory
UTAUT	Unified Theory of Acceptance and Use of Technology
TAM	Technology Acceptance Model
IT	Information Technology
SPSS	Statistical package for social sciences
IQR	Inter quartile range
PCA	Principal Component analysis
KMO	Kaiser Meyer-Olkin
VIF	Variance inflation factor
PE	Performance expectancy
EE	Effort expectancy
SI	Social influence
FC	Facilitating conditions
UP	User privacy
ANOVA	Analysis and Analysis of Variance
CI	Condition index

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

This chapter presents the theoretical research background the problem statement, purpose of the study and research questions. It also introduces the reader to the research objectives and subsequently, research questions and justification of the study.

1.1 Background

Accurate and automatic identification and authentication of users is a fundamental problem in network environments. Personal Identification Numbers or Passwords and key devices like Smart cards are not just enough in some cases. What is needed is something that could verify that you are physically the person you claim to be. (Koteswari et al, 2011). The use of biometric authentication has been identified as a solution for this problem.

Biometrics is usually integrated into security applications with the aim of strengthening security and curbing falsifications of identities. By definition, biometric authentication refers to technologies that measure and analyze human physical and behavioral characteristics for authentication purposes (Nanavati, Thieme &Nanavati 2002).

Substantial interest exists in biometric authentication technology and its application as a means of enhancing existing identity management systems, but there are also valid concerns when protecting the stored data (Wayman 2008). This poses a principal adoption decision for an organization because this type of authentication requires strict privacy measures, adequate database management, and a long-term financial commitment due to the sensitive nature of the data being stored (Laux 2011)

Because biometric technologies encompass a group of technologies designed to identify and validate the identity of individuals using one or more of their intrinsic and unique physical or behavioral traits (Bolle et al. 2004), it represents a robust technology for deterring fraudulent access to online, as well as on-site, financial services.

1.2 Problem Statement

While several biometric technologies have been widely used for a decade or more, limited research has examined biometrics adoption in organizations. Much of the research examining biometric adoption and use is descriptive and focuses on technology characteristics. No research has empirically examined the adoption of biometrics in a large, representative sample of organizations in one industry. Further, although several researchers have discussed the role of biometrics in security applications for financial institutions, no systematic empirical research has been applied to studying the role of organizational characteristics, contextual factors, and perceived benefits of the technology in this or related industries (Laux 2011).

Jones et al (2006) carried out research aimed at examining the factors affecting the adoption of biometric authentication technology using Technology Acceptance Model (TAM). The results of their research indicated that External Pressure and Readiness were both more important factors in the adoption decision than Perceived Benefits. However their research focused on the adoption factors from the management point of view whose adoption attitudes and need may have been influenced by the need for reduced financial frauds, regulatory requirements and increased profitability. Their study examined organizational considerations related to biometrics adoption, not customer attitudes about use of such technology.

1.3 OBJECTIVES

This research intends to achieve the following objectives:

1. To develop a framework for the adoption of biometric ATM authentication in the in the Kenyan financial institutions.
2. To apply the developed framework to study factors influencing adoption of biometric ATM authentication in the Kenyan financial institutions.
3. To validate the conceptual framework.

1.4 Research Questions

1. What is the effect of Performance expectancy on behavioral intention to adopt biometric ATM authentication
2. Do gender, experience and age have any moderating effect on performance expectancy in adoption of biometric authentication?
3. What is the effect of Effort expectancy on behavioral intention to adopt biometric ATM authentication.
4. Do usage experience, gender and age have any moderating effect on effort expectancy?
5. Is there any relationship between social influence and behavioral intention to adopt biometric ATM authentication?
6. What is the moderating power of experience, age and gender on social influence in the adoption of biometric ATM systems?
7. What is the effect of Facilitating conditions on the intention to adopt biometric ATM authentication?
8. Do age and experience have any moderating power on facilitating conditions on behavioral intention to adopt biometric ATM authentication?
9. Is there a direct relationship between user privacy and behavioral intention to adopt biometric ATM authentication?
10. Do experience, gender and age have any moderating effect on user privacy in the adoption of biometric ATM authentication?

1.5 Justification of Study

Breckenridge (2005) examined the deployment of biometric technology in South Africa. He suggests that before an organization embarks on an implementation plan of biometric system deployment, it would be wise to examine the lessons that can be learned from South Africa's troubled adoption of a biometric-based authentication system.

According to the media reports on the biometric voter registration system in Kenya's 2013 general elections, there were concerns about some of the adoption factors that the Independent Electoral and Boundaries Commission (IEBC) had not taken into consideration. Among them were privacy concerns where most of the citizens perceived the possibility of access of the biometric templates by a third party, in this case the Criminal Investigation department, CID and other investigative bodies. It is therefore important to have an adoption framework that takes care of all the adoption factors from the stakeholders. The validated framework can be further developed and refined to benefit other financial institutions that require user authentication.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

Information technology adoption by users is considered to be attributed to various drivers or factors that are interrelated. Various models have been put forth to facilitate the understanding of Information Technology adoption. In this chapter we will discuss the theoretical models and illustrate the key constructs of IT adoption that each model addresses.

2.2 Biometric Technology adoption Models

There are eight models that have been developed and used in earlier research to explain technology usage and behavior. These models are:

1. The Theory of Reasoned Action
2. The Theory of Planned Behavior
3. Innovation Diffusion Theory.
4. Social Cognitive Theory
5. Unified Theory of Acceptance and Use of Technology

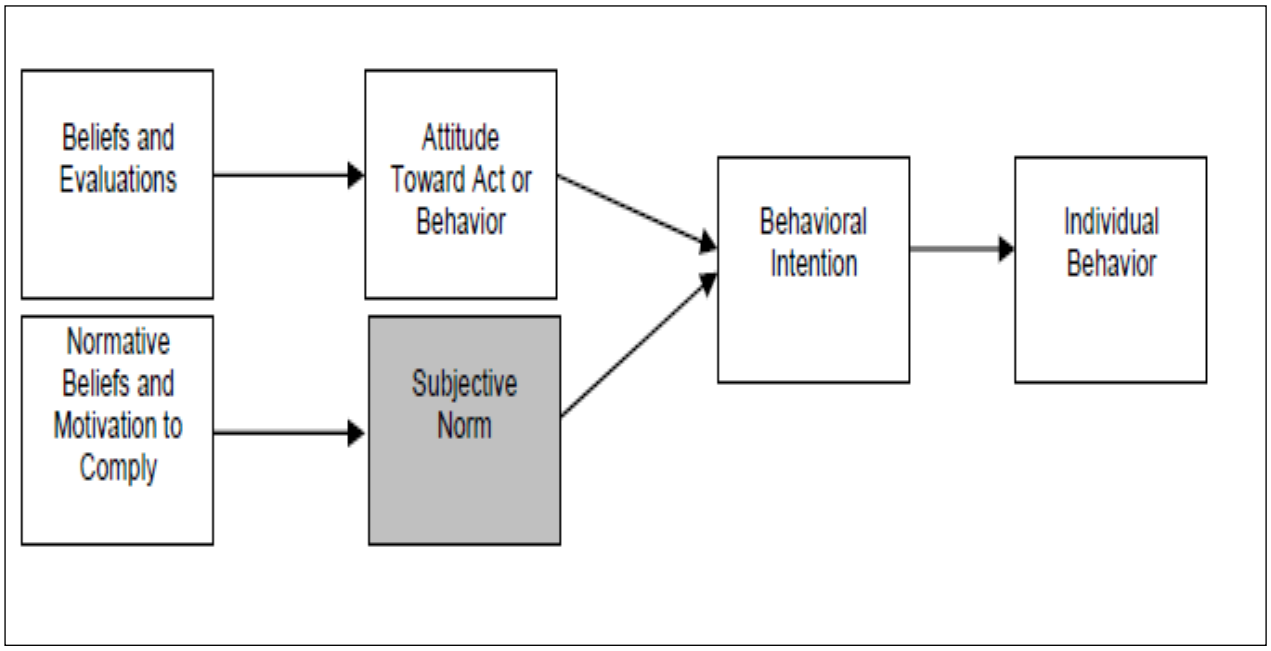
2.2.1 The Theory of Reasoned Action (TRA)

This model points out that an individual behaves in a manner which is in accordance with his or her intention to exhibit the behavior (Williams, 2009). Consequently, Behavioral Intention is driven by the person's Attitude towards a given Act or Behavior and their Subjective Norm.

Applied to adoption of biometric authentication by the financial service providers, TRA seems to maintain that, individuals would accept biometric authentication if they could see that there would be positive benefits or outcomes associated with using this technology. The TRA model is a widely studied model from social psychology concerned with the determinants of consciously intended behaviors. However the model does not pay tribute to other adoption drivers such as facilitating conditions offered by new technology, performance expectancy and effort expectancy

as well as cost. The model mostly attributes importance on social influence on intended behavior to adopt a system.

Figure 1: Theory of Reasoned Action Model



Source: **Fishbein et al**

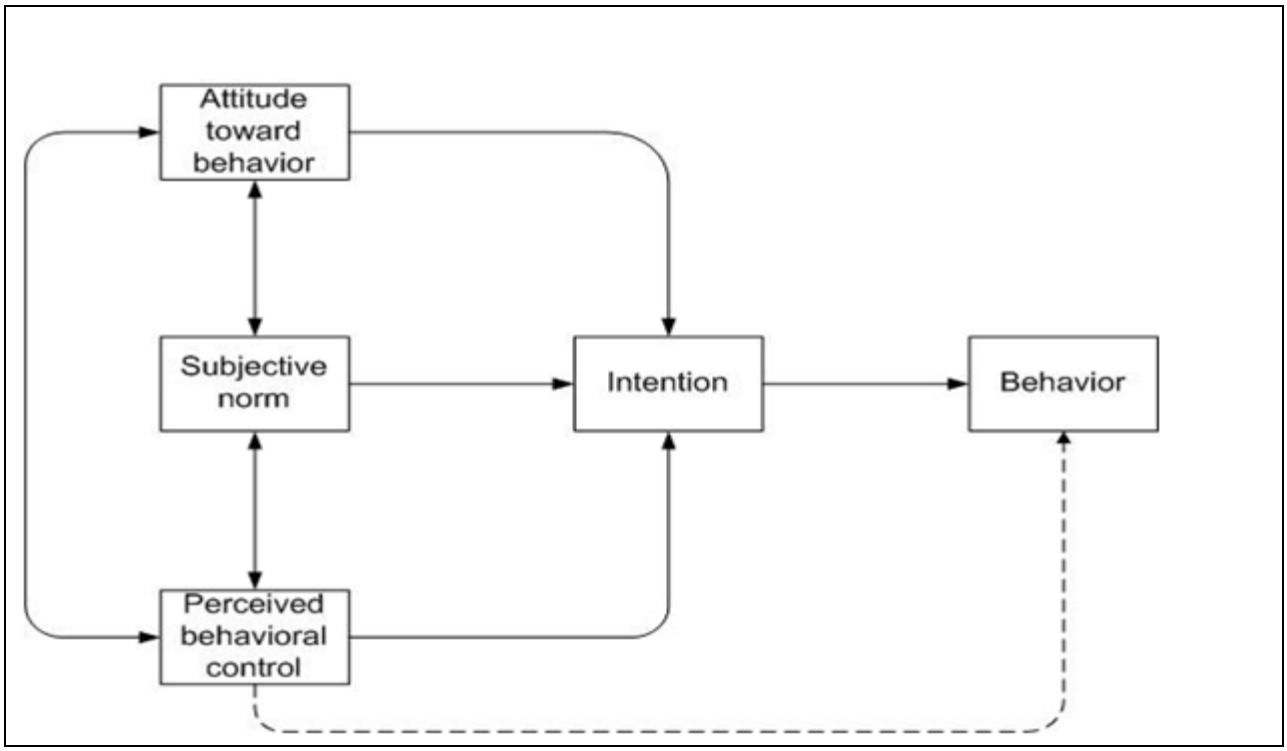
2.2.2 Theory of Planned Behavior (TPB) Model

This model explains posits behavioral intentions to be the driver of individual behavior towards adoption. TPB improves the predictive power of the theory of reasoned action by including perceived behavioral control. This could imply that an individual does not have a complete control of their behavior under certain conditions. Perceived Behavioral Control refers to the perceived ease or difficulty of performing or exhibiting behavior (Taylor and Todd, 1995)

The Decomposed Theory of Planed Behavior (DTPB) Model tends to improve on the weaknesses of TPB by providing a more comprehensive understanding of Behavioral Intention through a focus on factors that are likely to influence systems use through the application of both design and implementation strategies. The model examines the dimensions of Subjective Norm and Perceived Behavioral Control by decomposing them into specific belief dimensions. (Taylor and Todd, 1995)

According to DTPB, performance expectancy, social influence and facilitating conditions are seen as adoption drivers influencing behavioral intention and usage behavior but it fails to exhaust considerations of effort expectancy influence on behavioral intention.

Figure 2: Theory of Planned Behavior Model

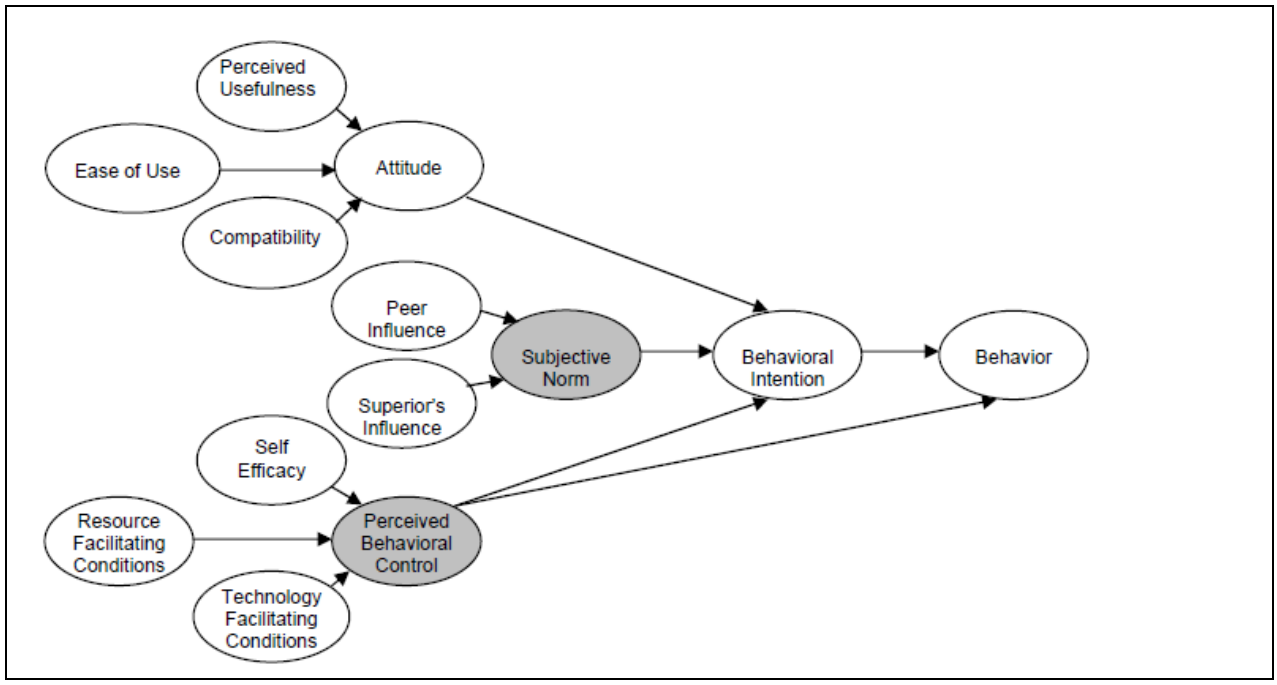


***Source*: Ajzen (1980)**

TPB focuses more on users' behavior towards adopting a system and does not consider design and implementation strategies of the system to be adopted.

The weaknesses of TPB were addressed by the Decompose Theory of Planned behavior, DTPB. DTPB aims to provide a more comprehensive understanding of Behavioral Intention through a focus on factors that are likely to influence systems use through the application of both design and implementation strategies. The strength of DTPB is its ability to identify specific beliefs that may influence IT usage.

Figure 3: Decomposed Theory of Planned Behavior Model



Source: Taylor and Todd, "Understanding Information Technology Usage," 146.

2.2.3 Innovation Diffusion Theory (IDT) Model

According to the IDT Model, there are five attributes of innovation that influence adoption namely;

1) Compatibility: The degree to which an innovation is perceived as being consistent with the existing values, past experiences, and needs of potential adopters.

2) Complexity: The degree to which an innovation is perceived as difficult to understand and use.

3) Observability: The degree to which the results of an innovation are visible to others.

4) Relative Advantage: The degree to which an innovation is perceived as being better than its precursor.

5) Trialability: The degree to which an innovation may be experimented with on a limited basis.

The model was developed to be used in terms of potential adopters use, trial or observation of the innovation rather than focusing on the innovation itself.

2.2.4 Social Cognitive Theory (SCT) Model

In this model, behavior, Personal, and Environmental influences operate interactively as determinants of each other.

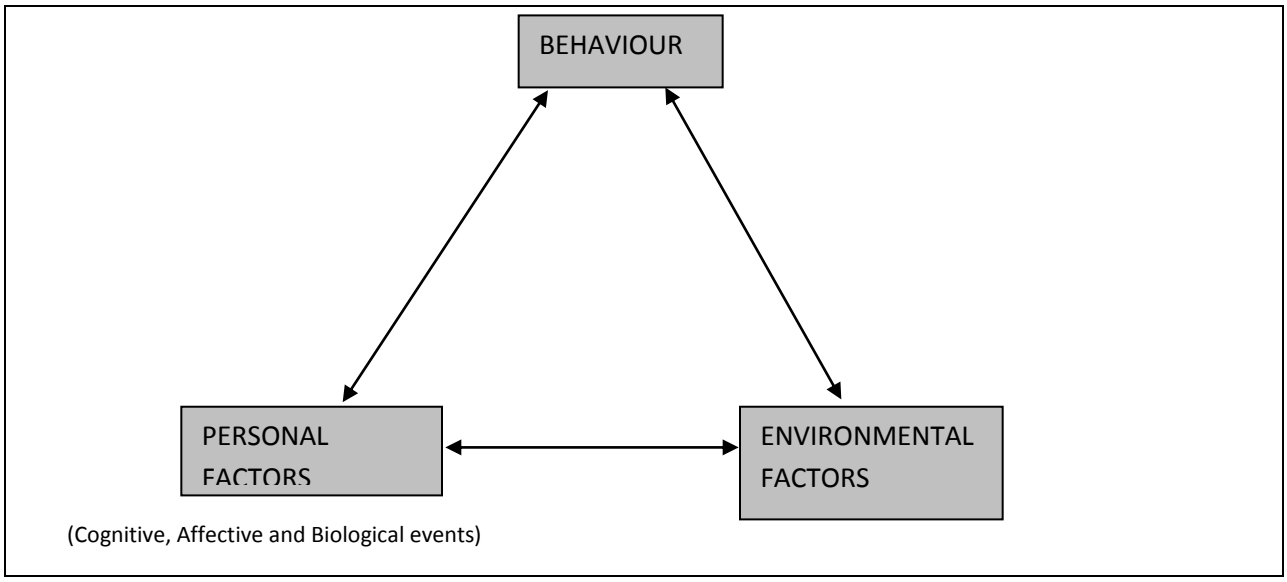


Figure 4: Social Cognitive Theory

2.2.5 Unified Theory of Acceptance and Use of Technology

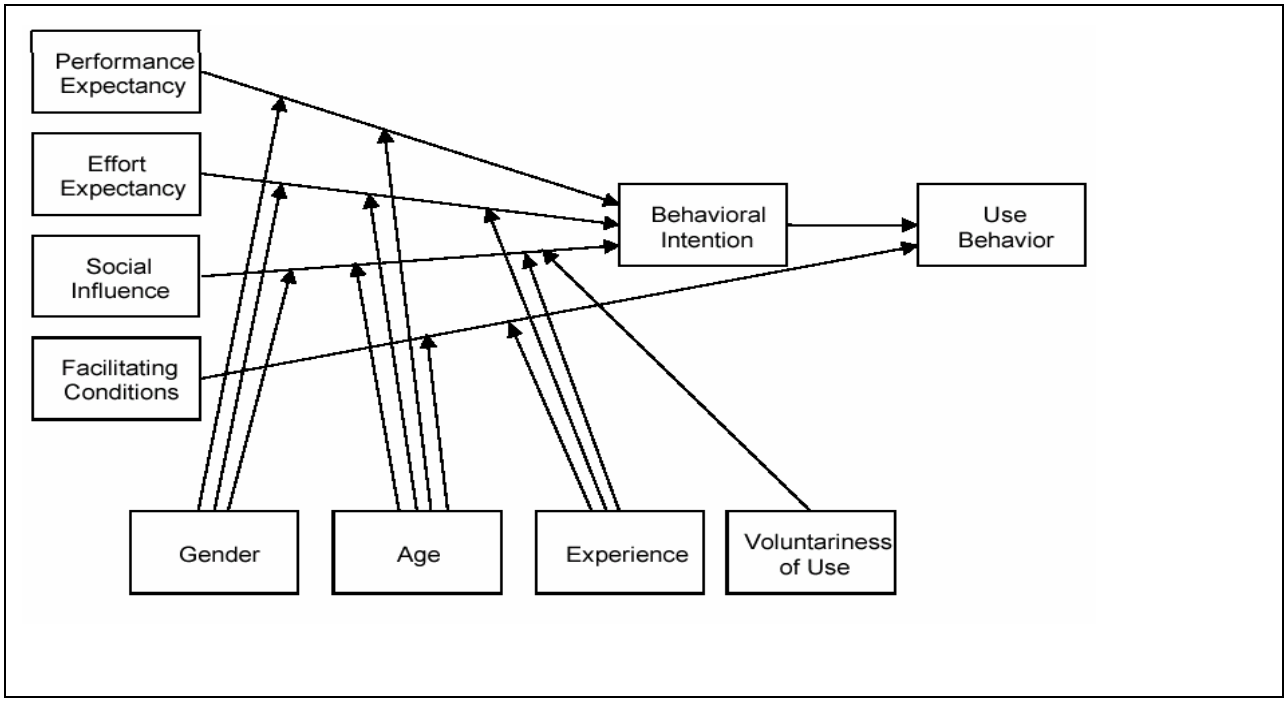
UTAUT considers four constructs hypothesized to have a significant role as direct determinants of user acceptance and usage behavior. The four constructs include; performance expectancy, effort expectancy, social influence and facilitating conditions.

The constructs are moderated by age, gender, experience and voluntariness of use to determine user acceptance and usage behavior such that;

- The influence of performance expectancy on behavioral intention is considered to be moderated by gender and age such that the effect is stronger for men and particularly the younger men.

- The influence of effort expectancy on behavioral intention is considered to be moderated by age gender and experience such that the effect is stronger for women, particularly the younger women and at early stages of experience.
- The influence of social influence on behavioral intention is considered to be moderated by age gender, experience and voluntariness of use such that the effect is stronger for women, particularly the older women in mandatory settings in early stages of experience.
- Facilitating conditions are considered not to have significant influence on behavioral intention but on use behavior.
- The influence of facilitating conditions on usage is considered to be moderated by age and experience such that the effect is stronger for older people, particularly with increasing experience.
- Behavioral intention is considered to have significant positive influence on usage.

Figure 5: UTAUT Model



***Source*: Venkatesh *et al.* (2003)**

2.3 Summary of the Gaps in the Reviewed Adoption models

This chapter has presented and discussed the literature on technology acceptance theories and models. There are however some shortfalls that are associated with their use in determining the adoption drivers of biometric ATM authentication. The gaps have been summarized in table 1 below.

Table 1: Summary of the Gaps in the Reviewed Adoption models

Model	Gaps
The Theory of Reasoned Action (TRA)	Does not pay tribute to other adoption drivers such as facilitating conditions offered by new technology, performance expectancy and effort expectancy as well as cost.
The Theory of Planned Behavior (TPB)	TPB focuses more on users' behavior towards adopting a system and does not consider design and implementation strategies of the system to be adopted.
Innovation Diffusion Theory.	The model was developed to be used in terms of potential adopters use, trial or observation of the innovation rather than focusing on the innovation itself
Social Cognitive Theory	Because social cognitive theory is so broad, it has been criticized for lacking any one unifying principle or structure.
Unified Theory of Acceptance and Use of Technology	Fails to address the issue of user privacy concern which is a key factor in the adoption of the biometric authentication systems.

2.4 THE CONCEPTUAL FRAMEWORK

This research identifies five factors that affect the adoption of the biometric authentication in the Kenyan financial service providers namely:

1. Performance expectancy
2. Effort expectancy
3. Social influence
4. Facilitating conditions
5. User privacy

Performance expectancy

This refers to the degree to which the stakeholders believe that using biometric authentication at the ATMs will help them improve transaction security.

Effort expectancy

Effort expectancy refers to the degree of ease associated with the use of biometric authentication at the cash dispensing machines.

Social influence

This is the importance to which an individual attaches others' believes on the use the biometric authentication systems at the bank ATMs.

Facilitating conditions

This is the degree to which an individual believes that the Kenyan financial service providers and technical infrastructure exists to support use of system or service. The compatibility of the new biometric systems with the current implementations is also considered here. This factor also looks at the cost of implementation, whether the bank directors and shareholders will be willing

to fund the implementation of the biometric authentication ATMs and the support that the users expect from the financial institutions.

User privacy

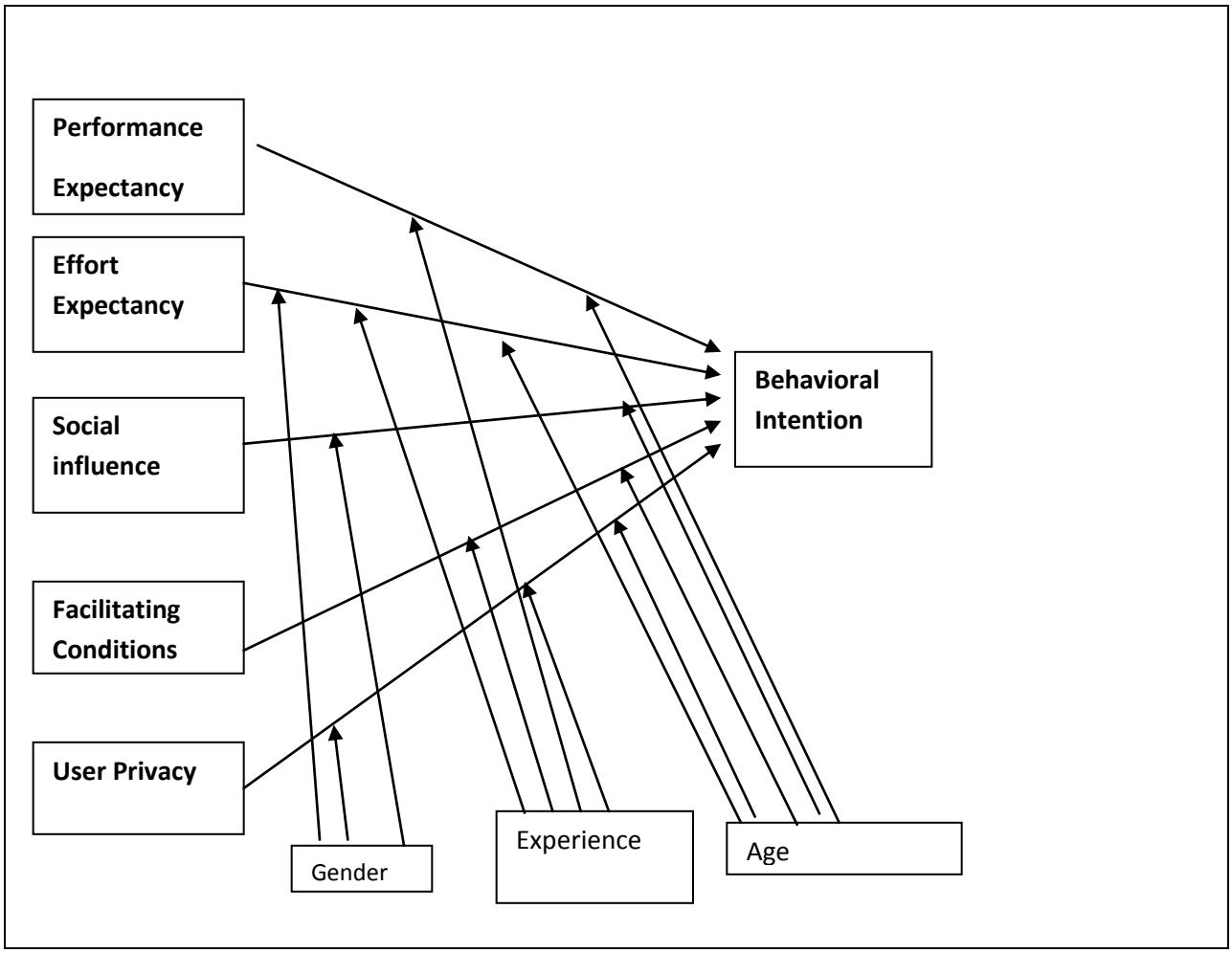
For the purposes of our study we will consider user privacy as a factor for the adoption of Biometric authentication in the Kenyan financial sector. The concerns on privacy of the biometric data during the enrollment stage and its storage of biometric data are major issues that can affect the adoption of this technology. It is therefore important to know the extent to which the customers are concerned about this factor.

Biometric data contains information acquired from individuals, which can be used to identify them. This raises issues of privacy and data protection. If the biometric data is recorded in a central database, privacy concerns may be higher than for systems where an individual's data is stored only on a card retained by the individual. Note however, that some biometric applications require a central database for their basic functionality e.g. to check for multiple enrolment attempts.

Customers may be concerned that their biometric data could be used for other purposes than it was originally acquired; for example, face image data might be used for surveillance purposes and fingerprint data checked against forensic databases. These concerns are at the heart of many objections to the use of biometrics. It is therefore necessary to understand privacy issues in regard to biometric data and biometric systems.

Having identified all these factors, the researcher came up with the conceptual framework depicted on figure 6.

Figure 6: The conceptual framework



Source: Author

2.5 Research Hypothesis

H1: Performance expectancy has a direct relationship with behavioral intention to adopt biometric ATM authentication and is moderated by usage experience and age.

H2: Effort expectancy has a direct effect on behavioral intention to adopt biometric ATM authentication and is moderated by usage experience, gender and age.

H3: Social influence has a direct relationship with behavioral intention to adopt biometric ATM authentication and is moderated by age and gender.

H4: Facilitating conditions have a direct effect on intention to adopt biometric ATM authentication and is considered to be moderated by experience and age.

H5: User privacy has a direct effect on behavioral intention to adopt biometric ATM authentication and is considered to be moderated by experience, gender and age.

CHAPTER 3: METHODOLOGY

3.1 Research Design

This study is conducted for the purpose of testing the hypothesis derived from the model presented. It is believed that studies employing hypothesis testing usually tend to explain the nature of certain relationships, or establish the differences among groups or the independence of two factors or more in a situation. Hypothesis testing offers an enhanced understanding of the relationships that exist among variables.

This research used a survey technique in the collection of data. Survey research uses scientific sampling and questionnaire design to measure characteristics of the population with statistical precision. The respondents were "randomly" sampled - that means that each person in the population has a known probability of being sampled.

There are defined techniques, such as random digit dialing and sampling procedures to ensure a scientific sample. The researcher used questionnaires and interviews as instruments of data collection.

Table 2: Summary of research design

Hypothesis	Variables	Data Collection	Materials and Instruments	Scale to be used	Data sources
H1	Performance Expectancy	Survey	Questionnaires	5 - point Likert - scale	Customers
H2	Effort Expectancy	Survey	Questionnaires	5 - point Likert - scale	Customers
H3	Social Influence	Survey	Questionnaires	5 - point Likert - scale	Customers
H4	Facilitating Conditions	Survey	Questionnaires	5 - point Likert - scale	Customers
H5	User Privacy	Survey	Questionnaires	5 - point Likert - scale	Customers

3.2 Target Population

The study's target population was the 1120 customers of Yetu Sacco which has already implemented the biometric ATM authentication. These customers were the suitable candidates for this research since they were conversant with the biometric authentication techniques and could therefore be able to give the required information.

3.3 Sample Size

Stratified sampling was employed during the research. This method is used when the parent population or sampling frame is made up of sub-sets of known size. These sub-sets make up different proportions of the total, and therefore sampling should be stratified to ensure that results are proportional and representative of the whole. In the case of this research, the subsets of known sizes were individual branches and several branches made up the significant percentage of the entire banking industry.

The rule of thumb was adopted for the study where for a small population of less than 1000, a sampling ratio of 30% is recommended for equal accuracy. A sampling factor of 0.3 was used to obtain the sample:

0.3*1120

= 336 respondents.

Table 5 gives a breakdown of the number of respondents from each branch.

Bank	**Branch Selected**	**Sample of respondents**
Yetu Sacco	Kinoro branch	80
	Kionyo branch	78
	Rubiri branch	78
	Nairobi branch	100
	TOTAL	**336**

Table 3: Breakdown of the Respondents

In each branch we looked at the factors which are which customers consider important in the adoption of the biometric authentication at the ATM systems.

3.4 Instrument development and design

The design of the research instrument consisted of two sections; part one covered the demographic characteristics of the respondents and part two covered the empirical measurements for the constructs in the conceptual framework.

The determinants in the conceptual framework were: Performance expectancy, Effort expectancy, Social influence, Facilitating conditions and User Privacy.

3.5 Pilot study

A pilot study involving 15 respondents was conducted to test the adequacy of the research instrument and to uncover potential problems for the main study. Reliability and validity tests were used as key determinants for the usefulness of the research instrument.

Each determinant had four to six questions. Factor analysis was employed to select two or three questions for every determinant. All scale questions were measured on a 5-point scale with points strongly disagree, disagree, neutral, agree and strongly agree.

3.6 Questionnaire Administration and Response rate.

The questionnaires were delivered by hand to the customers at the various branches. Each questionnaire was accompanied by an introductory letter explaining the purpose of the study. Among the distributed copies 260 were returned of which 240 were found usable for analysis. 20 were discarded since they were incomplete to an extent of being unusable for analysis. The overall response rate was 87%. The good response rate was due to the fact that rectification of a number of limitations observed during the pilot study and that the questionnaire wasn't unnecessarily long for the customers.

3.7 Data management

3.7.1 Data editing and coding

After collecting data, coding was required so that it could be stored using SPSS software version 15.0. Data was edited by checking and adjusting for errors, omissions, legibility and consistency in order to ensure completeness, consistency and readability of the data. This was done using frequency distribution in SPSS. Data was coded by assigning characters/numbers to each answer and edited before it was entered into SPSS. Each question or item in the questionnaire has a unique variable name, some of which clearly identify the information such as gender and age.

A coding sheet was used to keep information about how each variable was coded. It comprised a list of all variables in the questionnaire, the abbreviated variable names that were used in SPSS and the way in which the responses were coded. Screening and cleaning of data before data analysis stage was necessary to make sure that there was no errors at the stage of keying data due to, mainly, human errors. By using descriptive statistics in SPSS (such as frequency analysis) the data was screened by checking each variable to see if the score was out of range or for continuous variables, checking minimum, maximum, mean and standard deviation. After finding errors it was necessary to go back to the questionnaires to confirm the data before correcting the error in the data file.

3.7.2 Data management for multivariate analysis

Data management is necessary before data analysis. It is essential to examine the data by checking the data file for errors. Data was then cleaned to a most suitable format for multivariate analysis by using missing data analysis.

3.7.2.1 Missing Data Analysis

The responses from the questionnaires had already been filtered and only usable questionnaires were used in the data file, but some missing data values existed. The missing values analysis was done and produced the output below.

Table 4: Missing data analysis

There are no variables with 5% or more missing values. TTEST table is not produced.
There are no categorical variables. CROSSTAB is not produced.
There are no variables with 5% or more missing values. MISMATCH table is not produced.

Source: Research data 2014

Table 5: Univariate statistics

	N	Mean	Std. Deviation	Missing		No. of Extremes(a,b)	
				Count	Percent	Low	High
Gender	240	1.458	0.499	0.000	0.0	0.000	0.000
Age	240	2.750	0.885	0.000	0.0	0.000	16.000
Q1	240	5.108	1.239	0.000	0.0	5.000	0.000
Q2	240	4.271	1.219	0.000	0.0	0.000	0.000
Q3	240	4.246	1.087	0.000	0.0	19.000	0.000
Q4	240	3.738	0.982	0.000	0.0	.	.
Q5	240	4.058	0.811	0.000	0.0	.	.
Q6	240	3.871	0.865	0.000	0.0	.	.
Q7	239	3.552	0.924	1.000	0.0	3.000	0.000
Q8	240	4.000	0.964	0.000	0.0	19.000	0.000
Q9	239	3.933	0.928	1.000	0.4%	15.000	0.000
Q10	239	3.954	0.826	1.000	0.4%	.	.
Q11	240	3.663	1.062	0.000	0.0	5.000	0.000
Q12	240	2.358	1.061	0.000	0.0	1.000	13.000
Q13	240	4.188	0.486	0.000	0.0	.	.
Q14	240	4.300	0.587	0.000	0.0	0.000	0.000

Source: Research data 2014

3.7.2.2 Multivariate Outlier Analysis

This is the stage after missing data analysis with respect to examining the data before data analysis. Multivariate outlier analysis was tested using SPSS 15. It was necessary to calculate the Mahalanobis distance which is the distance of a particular case from the centroid of the remaining cases, where the centroid is the point created by the means of all the variables. Computation of the Mahalanobis measure revealed that there were no cases with outlier characteristics.

3.7.2.3 Multivariate Normality Analysis

Multivariate normality is the most fundamental assumption in multivariate analysis. Normality is the correspondence to the normal distribution which is the benchmark for statistical methods. Normal is used to describe a symmetrical, bell shaped curve, which has the greatest frequency of scores in the middle, with smaller frequencies towards the extremes.

Normality can be assessed by obtaining skewness and kurtosis values. Skewness indicates the symmetry of a distribution while kurtosis provides information about the peakedness of the distribution. Negative kurtosis indicates a flatter distribution while a positive kurtosis indicates a peaked distribution. A positive skewness indicates a distribution shifted to the left while a negative skewness reflects a shift to the right.

In general skewness of 1 indicates moderate skewness. Kurtosis values less than 1 are negligible, values from 1-10 indicate moderate non-normality while values greater than 10 indicate severe non-normality. The maximum skewness value in this research was 1.756 and maximum kurtosis was 9.045.

Table 6: Skewness and Kurtosis values

	Skewness		Kurtosis	
	Statistic	Std. Error	Statistic	Std. Error
Gender	0.168	0.157	-1.988	0.313
Age	1.756	0.157	3.767	0.313
Duration of ATM usage	-1.191	0.157	0.716	0.313
Frequency of ATM usage	0.404	0.157	-1.425	0.313
Biometric ATM is necessary in combating ATM fraud	-1.999	0.157	3.597	0.313
Less time is spent in biometric ATM	-1.725	0.157	2.702	0.313
Biometric ATM is easy to learn	0.644	0.157	-0.138	0.313
Biometric ATM is easy to use	-2.460	0.157	9.045	0.313
The enrollment process for biometric authentication is simple and easy	-0.948	0.158	1.137	0.314
Using Biometric ATM makes me feel better than those who don't use it	-1.555	0.157	3.735	0.313
My parents, siblings, friends and other relatives think Biometric ATM is better than other authentications	-1.489	0.157	4.037	0.314
Bank officials are available to offer help on Biometric ATM use when I need it	-0.770	0.157	0.604	0.314
I have a privacy concern in biometric ATM	-0.749	0.157	-0.442	0.313
I feel that a third party may gain access to the biometric data	1.001	0.157	0.392	0.313
I intend to continue using biometric at the ATM in the near future	0.425	0.157	0.338	0.313
I recommend other financial service providers to adopt biometric authentication at the ATM	-0.180	0.157	-0.586	0.313

***Source*: Research data 2014**

CHAPTER 4: FINDINGS AND DISCUSSIONS

4.1 Demographics and Descriptive Statistics

Gender

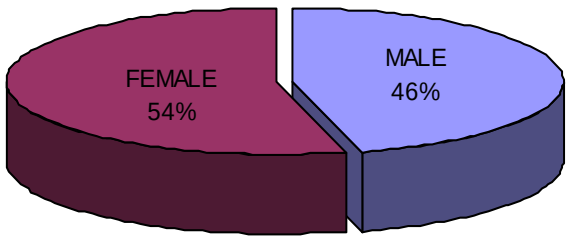
Demographic statistics on the data revealed that 54.2% of the population was male while 45.8% was female.

Table 7: Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	110	45.8	100.0	100.0
Missing	Male	130	54.2		
Total		240	100.0		

***Source*: Research data 2014**

Figure 7: Gender statistics



AGE

The majority of the respondents (47.1 %) were between the age of 31-40 years of age followed by 21-30years. 51-60 years constituted 4.2 percent while below 20 years was 2.9 percent.

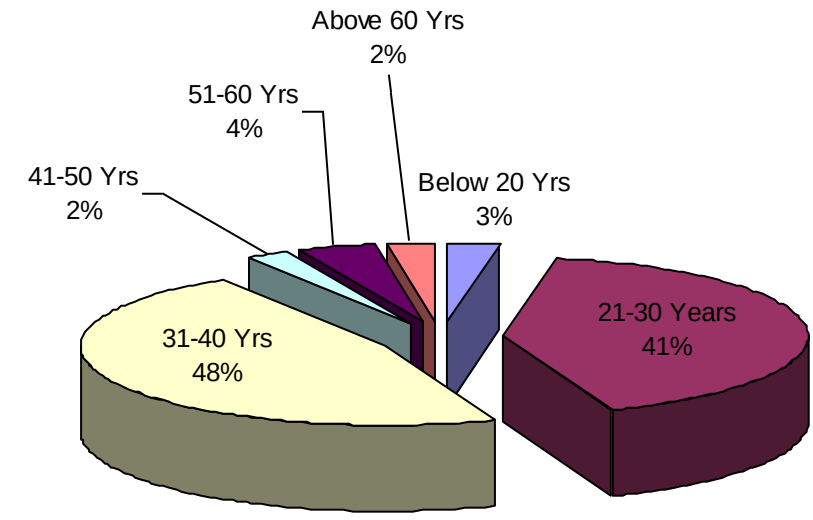
Table 8: Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Below 20 Yrs	7	2.9	2.9	2.9
	21-30 Years	99	41.3	41.3	44.2
	31-40 Yrs	113	47.1	47.1	91.3
	41-50 Yrs	5	2.1	2.1	93.3
	51-60 Yrs	10	4.2	4.2	97.5
	Above 60 Yrs	6	2.5	2.5	100.0
	Total	240	100.0	100.0	

***Source*: Research data 2014**

GENDER

Figure 8: The Gender demographics



EXPERIENCE

Table 9: Duration of ATM usage

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	<6 Months	5	2.1	2.1	2.1
	1-2 Years	24	10.0	10.0	12.1
	2-3 Years	50	20.8	20.8	32.9
	3-4 Years	17	7.1	7.1	40.0
	> 4 Years	144	60.0	60.0	100.0
	Total	240	100.0	100.0	

***Source*: Research data 2014**

Table 10: Frequency of ATM usage

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Weekly once	87	36.3	36.3	36.3
	Weekly Several Times	68	28.3	28.3	64.6
	monthly once	18	7.5	7.5	72.1
	Monthly several times	67	27.9	27.9	100.0
	Total	240	100.0	100.0	

***Source*: Research data 2014**

A large portion of the population (60%) had used the ATM for more than four years and uses it weekly once.

Figure 9: Duration of ATM usage chart

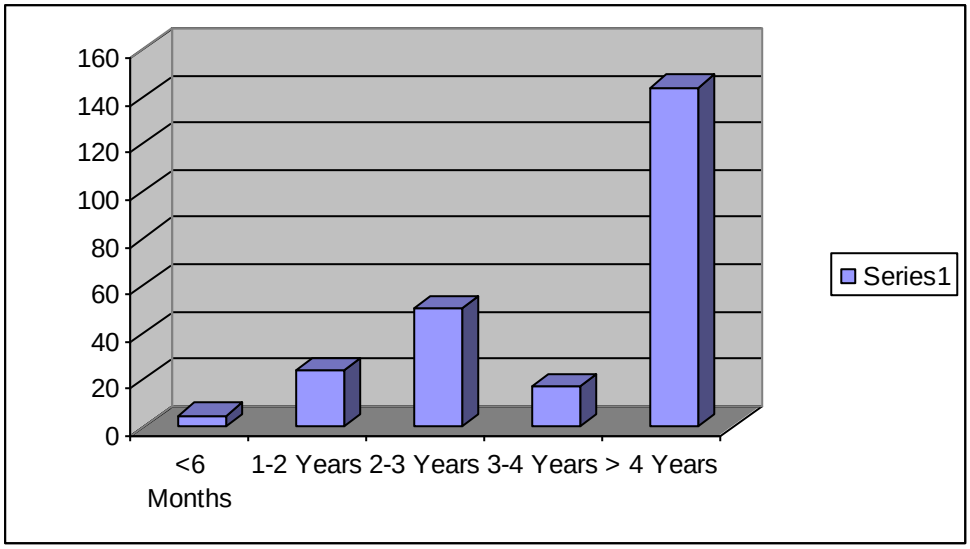
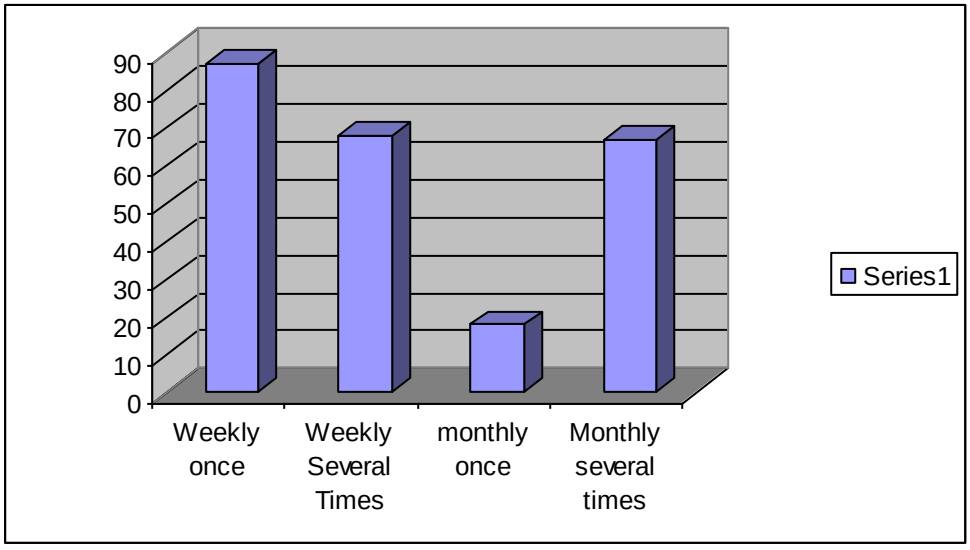


Figure 10: Frequency of ATM usage chart



4.2 Factor Analysis

Factor analysis is a statistical analysis approach that can be used to analyze interrelationships among large number of variables and to explain those variables in terms of their common underlying dimensions (factors). Factor analysis involves condensing of information contained in original variables into smaller set of dimensions with minimum loss of information.

This research used principal component analysis with verimax rotation to analyze the data using SPSS 15. The results comprised of tests carried out on quantitative data including Cronbach's Alpha and Factor Analysis.

4.2.1 Statistical Assumptions of Factor Analysis and Preliminary Analysis

i. Linearity

Factor analysis is a linear process so there needs to be a careful examination of any departures from linearity. Small sample sizes are vulnerable to non-linearity.

ii. Multivariate Normality

The dependent variables should be normally distributed for each combination of independent variables. The smaller the sample size, the more important it is to screen data for normality.

iii. Homoscedasticity

This was checked by testing the residuals and assuring that they were dispersed randomly throughout the range of the estimated dependent variable.

iv. No outliers

This research used Mahalanobis distance to identify cases which were multivariate outliers.

v. Factorability of correlation matrix

The researcher must look for correlations that are great than 3. If several values in the correlation matrix exceed 0.3 then it is appropriate to use factor analysis. The anti image correlation matrix is used to asses the sampling adequacy of each variable. Only variables with sampling adequacy of greater than 0.5 are included in the analysis. Both Bartlett's test of sphericity and Kaiser

Meyer-Olkin (KMO) measure of sampling adequacy can be used to determine the factorability of the matrix as a whole. If Bartlett's test of sphericity is significantly large among some of the variables, and Kaiser Meyer-Olkin index is greater than 0.6 then factorability is assumed.

vi. Absence of high Multicollinearity

Multicollinearity increases the standard error of factor loadings, making them less reliable and thereby making more difficult the process of inferring labels for factors. To detect Multicollinearity in factor analysis, KMO statistics may be used, or data first screened in regression analysis using Variance Inflation factor (VIF) or Tolerance. KMO and correlation matrix were used to detect Multicollinearity and collinear terms were eliminated prior to factor analysis.

vii. Adequate sample size

At a minimum there must be more cases than factors. The sample size of this research is 240 thus it meets the minimum cut off.

4.2.1.1 Reliability Analysis

Before to conducting factor analysis it was necessary to check reliability of the scale used to confirm that it used consistently reflected the variables being measured. Cronbach's Alpha was used to measure the scale of reliability.

Cronbach's Alpha value varies from 0-1, with higher values being desirable. The average Cronbach's Alpha for our data was 0.605.

The data under analysis has Cronbach's Alpha of 0.605 thus there it was within the acceptable reliability margins.

4.2.1.2 Kaiser Meyer Olkin (KMO) and Bartlett's Test of Sphericity

Kaiser Meyer Olkin (KMO) measures sampling adequacy while Bartlett's Test is a test of sphericity. Bartlett's Test examines the hypothesis that the group of variances is the same and dependent variables are uncorrelated in the population. The KMO statistic varies between 0-1. Values nearest 1 are desirable for factor analysis. It is also desirable that Bartlett's value $p<0.05$.

Table 11: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.556
Bartlett's Test of Sphericity	Approx. Chi-Square	1371.744
	df	45
	Sig.	.000

***Source*: Research data 2014**

The above results are acceptable the basis on which factor analysis was done.

4.2.2 Factor Extraction

Factor analysis was run on the sample. The extraction method used was principal component analysis (PCA) with varimax rotation method.

Table 12 below presents the results of the pricipal component analysis results.

Table 12: Factor Extraction

	Initial Eigenvalues(a)			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.227	17.179	17.179	2.227	17.179	17.179	1.621	12.504	12.504
2	1.891	14.583	31.762	1.891	14.583	31.762	1.780	13.727	26.231
3	1.635	12.612	44.374	1.635	12.612	44.374	1.767	13.630	39.861
4	1.545	11.916	56.290	1.545	11.916	56.290	1.298	10.011	49.872
5	1.214	9.367	65.657	1.214	9.367	65.657	1.404	10.829	60.701
6	0.991	7.642	73.298						
7	0.791	6.098	79.397						
8	0.683	5.269	84.665						
9	0.603	4.651	89.316						
10	0.385	2.966	92.282						
11	0.345	2.662	94.944						
12	0.194	1.497	96.441						
13	0.157	1.210	97.651						
14	0.129	0.992	98.644						
15	0.112	0.866	99.510						
16	0.064	0.490	100.000						

***Source*: Research data 2014**

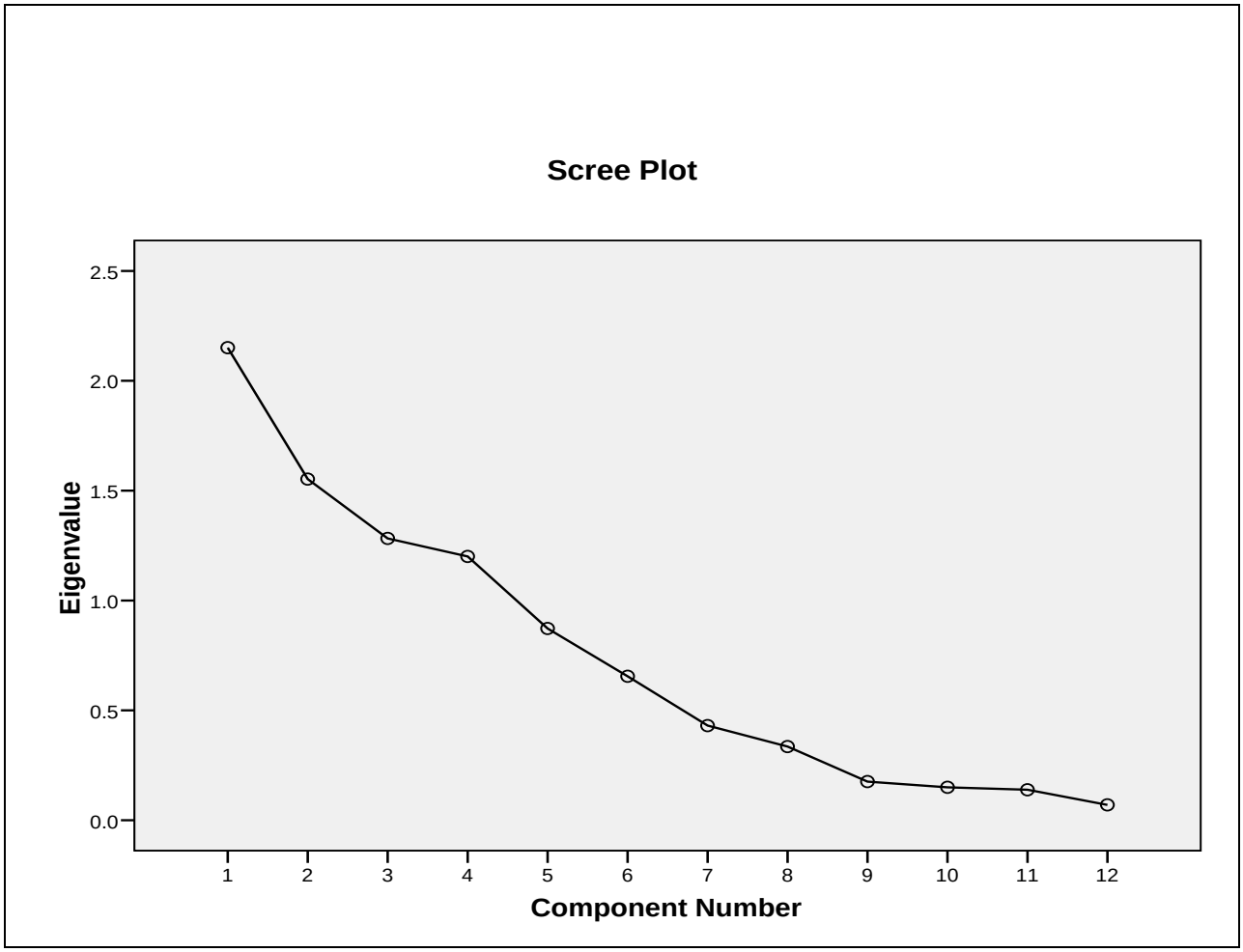
In running factor analysis not all factors are retained in the analysis. The eigenvalues associated with each factor represent the variance explained by that particular linear component and SPSS also displays the eigenvalues in terms of variance e.g. factor 1 explains 17.179 % of variance. SPSS extracts all factors with eigenvalues greater than 1 thus leaving 5 factors which are displayed in the columns labeled *Extraction Sums of Squared Loadings*. The values which are

not moved to the above column are discarded. The factors after rotation are displayed in the columns Rotation Sums of Squared Loadings. Rotation optimizes the factor structure thus the relative importance of the four factors is equalized.

This preliminary analysis therefore resulted in a solution of 5 factors selected for further analysis.

In addition to eigenvalues analysis, a scree plot inspection can also give a useful insight to the relative importance of each factor.

Figure 11: Scree Plot



***Source*: Research data 2014**

The cut off for selecting factors should be at the inflexion point of the curve. As seen in the scree plot above, the inflexion point is at component 4 which agrees with the eigenvalues table above.

4.2.3 Factor Rotation

The rotated component matrix was examined for items and the factors further tested with varimax rotation method. This resulted in the table below.

Table 13: Varimax rotation

	1	2	3	4	5
Performance Expectancy1	-0.340	0.228	0.962	0.017	-0.024
Performance Expectancy2	0.334	0.028	0.827	-0.025	0.075
Effort Expectancy1	0.070	0.087	-0.010	0.145	-0.014
Effort Expectancy2	0.603	0.001	0.167	0.262	0.138
Effort Expectancy3	0.486	0.117	0.157	0.575	0.049
Social Influence1	0.047	0.869	0.099	0.087	0.030
Social Influence2	0.019	0.875	0.070	0.024	-0.043
Facilitating conditions1	-0.132	0.104	-0.123	0.095	-0.113
User Privacy1	0.007	0.002	0.033	-0.098	1.056
User Privacy2	0.376	0.130	0.123	-0.934	0.187
Behavioral intention1	0.276	0.021	-0.010	0.000	-0.033
Behavioral intention2	0.373	0.011	-0.023	-0.050	0.022

***Source*: Research data 2014**

Normally researchers accept a loading of an absolute value of more than 0.3 to be important. Where the scale has an acceptable loading on more than one component, one of these loadings can be reduced to the component with the highest value. Eg Effort Expectancy3 is loaded on

component 1 (0.486) and 4 (0.575), therefore the loading on component 1 is eliminated since it is less than component 4.

Table 14: Scale for factor rotation

Performance Expectancy1	Biometric ATM is necessary in combating ATM fraud
Performance Expectancy2	Less time is spent in biometric ATM
Effort Expectancy1	Biometric ATM is easy to learn
Effort Expectancy2	Biometric ATM is easy to use
Effort Expectancy3	The enrollment process for biometric authentication is simple and easy
Social Influence1	Using Biometric ATM makes me feel better than those who don't use it
Social Influence2	My parents, siblings, friends and other relatives think Biometric ATM is better than other authentications
Facilitating conditions1	Bank officials are available to offer help on Biometric ATM use when I need it
User Privacy1	I have a privacy concern in biometric ATM
User Privacy2	I feel that a third party may gain access to the biometric data
Behavioral intention1	I intend to continue using biometric at the ATM in the near future
Behavioral intention2	I recommend other financial service providers to adopt biometric authentication at the ATM

***Source*: Research data 2014**

4.2.4 Validation of factor analysis results

The research examined if the factor model is stable and generalizable and if the factor solution is impacted by outliers. Stability was examined by splitting the sample into two in order to see it

factor structure and commonalities remain the same. The data file had 240 respondents thus splitting the sample into two halves resulted to more than 50 cases each which is the minimum.

4.2.4.1 Comparison of the communalities of the two validation samples

A comparison was made on the two splits created above. While the communalities differed for the two models, in all cases they were above 0.3, indicating the factor model is explaining more than half of the variance in all the original variables.

Table 15: Component Matrix (a) SPLIT 1

	1	2	3	4	5
Performance Expectancy1	0.198	0.683	-0.015	-0.261	0.437
Performance Expectancy2	0.576	0.388	-0.502	-0.123	0.321
Effort Expectancy1	0.412	-0.055	0.507	-0.342	0.116
Effort Expectancy2	0.791	-0.114	-0.283	-0.151	-0.084
Effort Expectancy3	0.709	-0.038	-0.071	-0.380	-0.248
Social Influence1	0.350	0.601	0.415	0.179	-0.240
Social Influence2	0.257	0.572	0.544	0.277	-0.189
Facilitating conditions1	-0.069	-0.184	0.305	-0.150	0.632
User Privacy1	0.312	0.133	-0.520	0.203	-0.196
User Privacy2	0.168	0.111	-0.172	0.810	0.347
Behavioral intention1	0.657	-0.504	0.220	0.199	0.106
Behavioral intention2	0.644	-0.492	0.218	0.275	0.052

***Source*: Research data 2014**

Table 16: Component Matrix (a) SPLIT 1

	1	2	3	4
Performance Expectancy1	0.363	-0.252	0.563	-0.394
Performance Expectancy2	0.523	0.095	0.521	-0.564
Effort Expectancy1	0.382	-0.046	-0.528	0.201
Effort Expectancy2	0.546	0.427	-0.289	-0.254
Effort Expectancy3	0.539	-0.097	-0.509	-0.255
Social Influence1	0.730	-0.493	0.187	0.358
Social Influence2	0.730	-0.493	0.187	0.358
Facilitating conditions1	-0.038	-0.508	-0.267	0.211
User Privacy1	-0.099	0.233	0.366	0.475
User Privacy2	0.056	0.462	0.601	0.353
Behavioral intention1	0.466	0.584	-0.191	0.143
Behavioral intention2	0.412	0.738	-0.082	0.204

***Source*: Research data 2014**

The two rotated factor matrices for each split of the sample produced a similar pattern of loadings for both validation analysis of the complete sample apart. However component matrix split 1 included facilitating condition which was not included in sample 2 as well as in the complete sample.

4.2.5 Interpretation of the factors

Four of the conceptual framework variables are supported by results of factor analysis. These variables include:

- Performance expectancy
- Effort expectancy
- Social influence
- User privacy.

Normally researchers accept a loading of an absolute value of more than 0.3 to be important. The above factors loaded absolute values of more than 0.3 except **Facilitating conditions** whose maximum loading was 0.104. Therefore Facilitating conditions were not considered as a factor for further analysis.

4.3 Multiple Regression Analysis

Regression analysis is a statistic technique used to investigate the relationships between a dependent variable and one or more independent variables. Multiple linear regression is used in this study investigate the relationship between the behavioral intention and the four independent variables.

Regression coefficients can be used to evaluate the strength of the relationship between the independent variable and the dependent variable. R^2 value provides a measure of the predictive ability of the model. The close the R^2 value to 1 the better the regression equation fit to the data.

The F test is used to test the significance of the regression model as a whole. F is a function of R^2, the number of independent variables and the number of cases. F is computed with k and (n-1) degrees of freedom, where k = number of terms in the equation not counting the constant (Garson, 2008). The decision rule for F-ratio is to reject the null hypothesis if F is greater than the critical value of an appropriate level of significance, and not to reject the null hypothesis when F value is smaller or equal to the critical value of an appropriate level of significance.

Multiple regression analysis was used in this study to test the research hypothesis. The regression model can be presented as follows;

BI=a+b1PE+b2EE+b3SI+b4UP +e

Where

BI=behavioral intention

PE=performance expectancy

EE=effort expectancy

SI=Social Influence

US=User Privacy

a= the constant where regression intercepts the y axis

b= regression coefficients

e = random error

4.4 Assumptions for Regression Analysis and Analysis of Variance (ANOVA)

Before applying regression analysis and ANOVA, the following assumptions were tested to make sure the properness of the analysis.

Absence of outliers

Generally an outlier whose standardized residual is greater than 3.3 should be dropped from all regression models. The data file had the 2.0 as the greatest standardized residual.

Linearity

Examining the residual scatter is the most common way to identify any nonlinear patterns in the data. The scatter plot of standardized residuals versus the fitted values was visually inspected. The plots did not reveal any non linear patterns in the data indicating a linear relationship in all the regression models in this study.

Tolerance and Multicollinearity

Tolerance $=1-R^2$

Where R^2 is the multiple R of a given dependent variable regressed on all other independent variables.

If the tolerance value is less than 0.20, the independent should be dropped from the analysis due to Multicollinearity.

Variance Inflation Factor (VIF)

This is the reciprocal of tolerance. When VIF is greater than 4.0, Multicollinearity is the problem. VIF values below 10 indicate that Multicollinearity is not a problem.

Condition index

Many researchers suggest condition indexes over 15 indicate possible Multicollinearity and over 30 indicate serious Multicollinearity problems.

Table 17: Multicollinearity Test

DEPENDENT VARIABLE	INDEPENDENT VARIABLES	TOLERANCE	VIF	CI
Behavioral Intention	Performance Expectancy	0.677	1.478	10.044
	Effort Expectancy	0.636	1.583	17.887
	Social Influence	0.350	2.856	15.814
	User Privacy	1.000	1.000	4.770
Behavioral Intention	Age	1.000	1.000	6.387
	Performance expectancy and age	0.783	1.321	10.314
	Experience			
	Performance expectancy and experience	0.798	1.299	11.838
Behavioral Intention	Effort expectancy			
	Experience	0.996	1.004	9.202
	Gender	1.000	1.000	6.020
	Effort expectancy and experience	0.720	1.457	18.669
	Effort expectancy and age	0.937	1.068	14.116
	Effort expectancy and gender	0.952	1.050	14.129
Behavioral Intention	Social Influence and age	0.563	2.244	14.736
	Social Influence and gender	0.563	2.249	14.526
Behavioral Intention	User Privacy and experience	0.997	1.003	8.936
	User Privacy and gender	0.634	0.701	4.344
	User Privacy and age	0.998	1.002	6.445

***Source*: Research data 2014**

Normally distributed Error term

A histogram and a normal probability (P-P plot) are the methods to use to asses whether the error terms are normally distributed. This research tested normality using these two methods.

Independent error terms (No autocorrelation)

Uncorrelated error term in a data set means the current values should not be correlated with previous values. I.e. for any two observations within the data series, it's assumed that knowing one observation treatment tells nothing about the other observation**.** Dubin-Watson coefficient tests auto-correlation.

Dubin-Watson values range from 0-4, close to 0 indicates extreme positive autocorrelation; close to 4 indicates extreme negative autocorrelation and close to 3 indicates no serial autocorrelation (Garson, 2008) Durbin-Watson values should be between 1.5 and 2.5 to indicate independence of observations. Positive autocorrelation means standard errors of the beta coefficients are too small while negative autocorrelation means standard errors are too large. (Garson, 2008)

The tested Dubin-Watson values are summarized in the table 18.

Table 18: Independent error terms test

DEPENDENT VARIABLE	INDEPENDENT VARIABLES	DURBIN-WATSON VALUE
Behavioral Intention	Performance Expectancy	1.899
	Effort Expectancy	1.243
	Social Influence	1.754
	User Privacy	1.583
Behavioral Intention	Performance expectancy and age	1.928
	Performance expectancy and experience	2.1635
	Performance expectancy and awareness	11.784
Behavioral Intention	Effort expectancy and experience	1.935
	Effort expectancy and age	1.7935

	Effort expectancy and awareness	1.175
Behavioral Intention	Social Influence and age	1.92
	Social Influence and gender	1.9875
	Social Influence and awareness	1.501
	Social Influence and experience	1.675
Behavioral Intention	User Privacy and experience	2.285
	User Privacy and gender	2.0665
	Transaction duration and age	1.98895

***Source*: Research data 2014**

4.4.1 Hypothesis Testing

4.4.1.1 Testing for Direct Effects

There are four independent variables, Performance expectancy, effort expectancy, social influence and user privacy in the regression model. These factors were regressed against behavioral intention and provided the results in the table below.

Table 19: Testing for direct effects

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
performance expectancy	0.012	0.036	0.018	0.002	0.032
Effort expectancy	0.128	0.046	0.176	2.720	0.192
Social influence	0.007	0.038	0.012	0.115	0.373
User Privacy	0.013	0.020	0.028	0.422	0.171

Source: Research data 2014

All independent variables obtained positive beta weights hence have positive effect on the adoption of Biometric ATM authentication. Effort expectancy (ß=0.176) has the most influential

effect on behavioral intention, followed by user privacy (ß=0.0.028), Performance expectancy (ß=0.018) and lastly social influence (ß=0.012)

4.4.1.2 Testing Moderating Effects.

The statistics that describe the moderating effect include beta weights and multiple R-square. These values are presented for each product term that represents a moderating effect.

With respect to interaction variables, the relationships are measured by Beta values, which represent the strength of the relationship. The Beta for the interaction of the moderator with the variable provides information regarding the interaction effect.

The Beta values should not be less than 0.1 and if they go beyond 1, there is a sign of Multicollinearity. The scale for Beta values is as follows:

- If the Beta value is between 0.1 and 0.3, there is small effect
- If the value is 0.3 and 0.50 there is a medium effect
- Above 0.50 denotes a large effect
- Less than 0.1 denotes lack of effect on the variable

Table 20: The moderating effect of gender

	R^2	beta	sig
PE*GENDER	0.057	-0.037	0.007
EE*GENDER	0.210	0.100	0.140
SI*GENDER	0.023	-0.028	0.358
UP*GENDER	0.032	-0.018	0.166

Source: Research data 2014

According to the results above, gender has no effect on performance expectancy (beta=-0.037), Social influence (beta=0.028) and user privacy (beta=0.018).It however had a slight effect on effort expectancy (beta=0.100).

Table 21: The moderating effect of age

	R^2	beta	sig
PE*AGE	0.030	-0.005	0.156
EE*AGE	0.199	0.133	0.209
SI*AGE	0.006	-0.004	0.568
UP*AGE	0.021	0.005	0.250

Source: Research data 2014

Age has beta values of -0.005 on performance expectancy, -0.004 on social influence, and 0.005 on user privacy. Age only moderates effort expectancy with a beta value of 0.133

Table 22: The moderating effect of experience

	R^2	beta	sig
PE*EXPERIENCE	0.161	0.107	0.055
EE*EXPERIENCE	0.297	0.180	0.033
SI*EXPERIENCE	0.159	0.156	0.292
UP*EXPERIENCE	0.162	0.144	0.204

Source: Research data 2014

Experience has beta values of 0.107 on performance expectancy, 0.180 on effort expectancy, 0.156 on social influence and 0.144 on user privacy. Experience therefore moderates all these factors since it has beta values more than 0.100.

4.4.1.3 Testing for high order interaction effects

The moderators were examined further for high order interaction effects since all the moderators did not have two way interactions on all the variables.

Table 23: High order interaction effects

	beta
PE *EXPERIENCE	0.107
EE *EXPERIENCE*AGE*GENDER	0.090
SI*EXPERIENCE	0.156
UP *EXPERIENCE	0.144

Source: Research data 2014

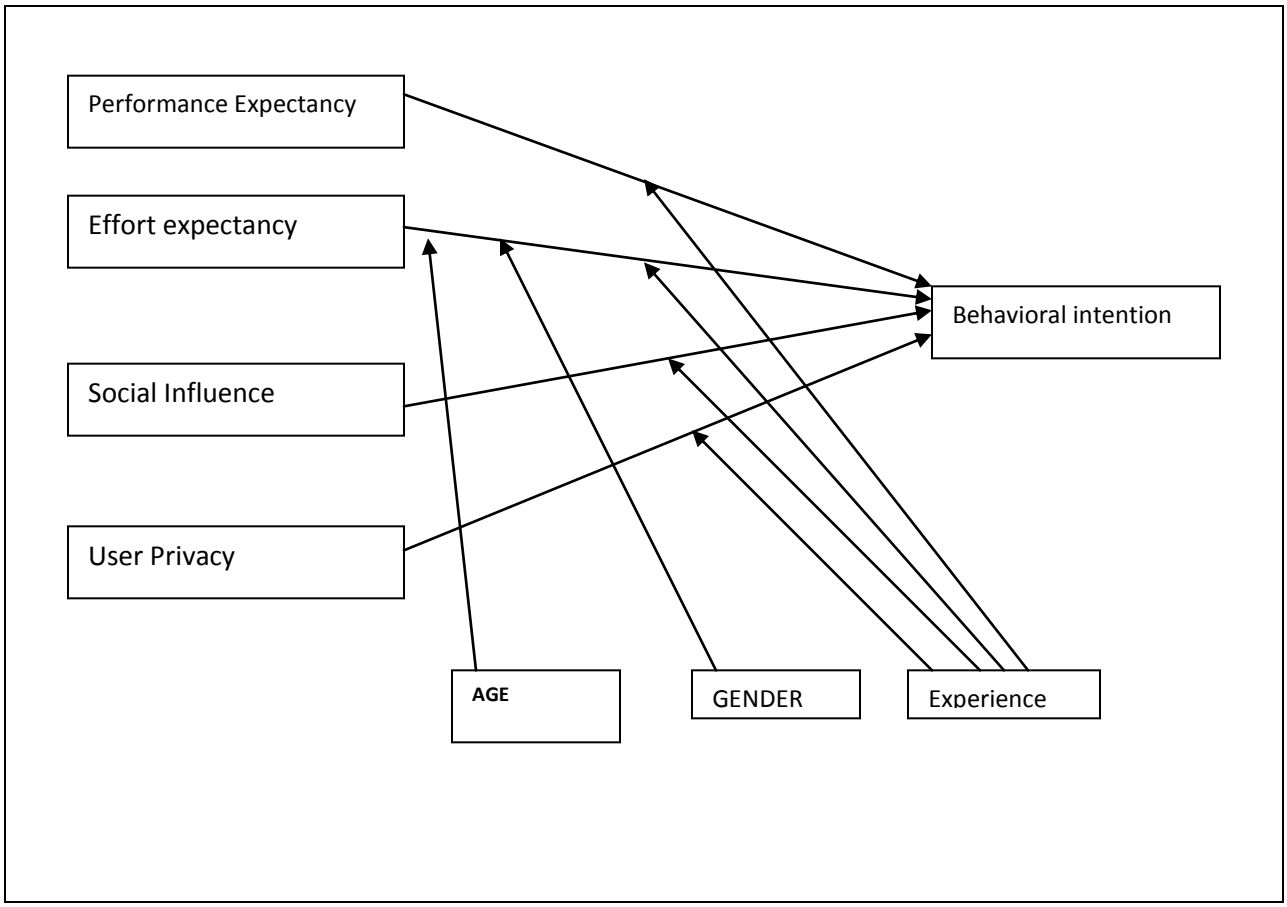
From the results of for high order interaction test, there were significant interactions between the moderators and the independent variables.

4.5 The Resulting Model

A model was derived that identified five factors that have a relationship with behavioral intention in the adoption of biometric ATMs. These variables were:

1. Performance expectancy moderated by experience
2. Effort expectancy moderated by gender age and experience
3. Social influence moderated by experience
4. User Privacy moderated by experience

Figure 12: The Resulting model



Source: Research data 2014

4.6 Model Discussion

This study intended to test the following hypothesis:

H1: Performance expectancy has a direct relationship with behavioral intention to adopt biometric ATM authentication and is moderated by usage gender, experience and age.

H2: Effort expectancy has a direct effect on behavioral intention to adopt biometric ATM authentication and is moderated by usage experience, gender and age.

H3: Social influence has a direct relationship with behavioral intention to adopt biometric ATM authentication and is moderated by experience, age and gender.

H4: Facilitating conditions have a direct effect on actual usage of biometric ATM authentication and is considered to be moderated by experience and age.

H5: User privacy has a direct effect on actual usage to adopt biometric ATM authentication and is considered to be moderated by experience, gender and age.

However the research found out the following

For H1, performance expectancy has a direct relationship with behavioral intention and is only moderated by experience. Age and gender were not found to have any moderating effect on performance expectancy.

For H2, effort expectancy was found to have a direct effect on behavioral intention and is moderated by age, gender and experience.

For H3, social influence was found to have a direct effect on behavioral intention to adopt biometric ATMs and is moderated by experience. Age and gender were found not to have any moderating effect on social influence.

For H4, facilitating condition was not loaded as a factor in the adoption of behavioral intention, thus H4 failed.

For H5, user privacy was found to have a direct effect on behavioral intention and is moderated by experience.

CHAPTER FIVE: RESEARCH CONCLUSIONS AND IMPLICATIONS

This project presented and discussed the findings of a study that focused on the factors affecting the adoption of biometric ATMs in the Kenyan financial service providers . The background of the study providing the general introduction and definition of the research problem was presented in chapter one while chapter two focused on the literature related to the study. The research methodology detailing sampling procedures and data collection methods employed by the study was presented in the third chapter. The fourth chapter focused on the statistical procedures and their interpretation, presentation and discussion of the research findings.

5.1 Research Conclusions

Here the researcher presents how the current research objectives have been achieved. A research model was developed and validated. Based on this research model, the study established that performance expectancy, effort expectancy, social influence and user privacy were key determinants for biometric ATMs acceptance adoption and usage in the Kenyan Financial service providers. In an organizational setting, the management needs to increase performance expectancy, reduce effort expectancy, increase the 'hype' of using biometric ATMs and assure the customers that the biometric templates will only be used for the purpose that they were intended to. Facilitating conditions factor was not found to be having any effect on behavioral intention to use biometric ATMs.

The study further demonstrated that age, gender and experience were moderating factors on effort expectancy. Experience was a moderating factor on performance expectancy, effort expectancy, social influence and user privacy.

5.2 Research Limitations

Venkatesh et al (2003), points out that acceptance models examine technology from the time of their initial introduction to stages of greater experience. The responses in this research have been collected and examined to measure perceptions and expectations after the participants' acceptance or rejection decisions rather than during active biometric ATM adoption decision-making process.

5.3 Contributions to Knowledge

This research expands knowledge in the area of biometric applications' adoption and usage. Identifying the adoption drivers of such applications helps researchers and stakeholders to design training, marketing and infrastructure support to encourage biometric applications acceptance. The ATM networks for the financial service providers are spread all over the country. For the current ATMs to be replaced much investments have to be made and if they are to recoup these investments, then these ATMs must be accepted and be used by the customers. Only by understanding the barriers to user acceptance of this technology can the financial service providers reduce those impediments.

This research identifies factors that are likely to affect the adoption of biometric ATM systems in the Kenyan banking sector. A clear understanding of these determinants will enable financial service providers to develop suitable marketing strategies, business models, processes, awareness programs and pilot projects

In conclusion, this study has contributed to knowledge with respect to theoretical extension and practical implementations. The validated framework can be further developed and refined to benefit other financial institutions that require user authentication.

5.4 Recommendations for Future Research

The application of biometric technology is wide. There are several types of biometrics that can be used at the ATM. The most common are finger print recognition, finger vein recognition, iris recognition, biometric hand geometry and facial recognition. This research focused on the general adoption of biometric ATMS and did not narrow down on the type of biometric authentication that can be used by the Kenyan financial service providers . There is therefore need to future researchers to find out the type of biometric that will be appropriate to the users.

APPENDIX 1: REFERENCES

Ajzen. I.1991). The theory of planned behaviour, *Organizational behaviour and Human Decision Process* 50(2): 179-211.

Breckenridge, K. 2005, The biometric state: The promise and peril of digital government in the new South Africa, *Journal of Southern African Studies* 31(2):267–282.

Corcoran, 'D., Sims, D., & Hillhouse, B., (2000). *Smart Cards and Biometrics: Your Key to PKI,* Retrieved [On-Line] http://0.....1inuxjoUfila1.cotI1l1jissue49/30 13.

Davis F.D., 1986. Technology Acceptance Model for Empirical Testing of New End User Information System: Theory and Results. Cambridge, MA: MIT Sloan School of Management.

Fishbein M. and Azjen, I, 1975. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison Wesley.

Gaur S., Shah V., Thakke M., 2012, Biometric Recognition Techniques: A Review, *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering* Vol. 1, Issue 4, October 2012.

Koteswari S., Paul J., Kumar V., Manohar A., 2011, A Method for fingerprint authentication for ATM based banking application, (IJCSIS) *International Journal of Computer Science and Information Security*, Vol. 9, No. 9, September 2011.

Laux D. , Luse A. , Mennecke B. Townsend A, , 2011, Adoption of Biometric Authentication Systems: Implications for Research and Practice in the Deployment of End-User Security Systems, *Journal of Organizational Computing and Electronic Commerce*, vol. pg 221–245.

Legris P., Ingham J., Collerette P., (2003) Why do people use information technology? A critical review of the technology acceptance model, *Information and Management* vol. 40 pg 191–204

Nanavati, S., Thieme, M. & Nanavati, R. 2002. *Biometrics: Identity Verification in a NetworkedWorld,* Toronto: John Wiley & Sons.

Taylor S. and Todd P., 1995b. Understanding Information Technology Usage. A Test of competing models, *Information systems Research* 6(2): 144-176

Tomi D., Niina M., Anssi O., 2008, Trust enhanced technology acceptance model- consumer acceptance of mobile payment solutions

Venkatesh, V., Morris, M., Davis, G., Davis F. (2003) User acceptance of information technology: toward a unified view. *MIS Quarterly*, (27)3, pp. 425-478.

Wayman, J. L. 2008, Biometrics in identity management systems, *IEEE Security and Privacy Magazine* 6(2) 30–37.

APPENDIX 2: QUESTIONNAIRE

Dear Respondent,

I am a student at University of Nairobi. I am carrying out a research project aimed at developing a framework for Biometric ATM authentication for the Kenyan Financial service providers . This research project is in partial fulfillment for the award of Master of Science in Information Systems. Your cooperation in completing this questionnaire as objectively and accurately as possible will be highly appreciated. This information will be kept in strict confidence and will only be used for the purposes of this research.

A. PERSONAL DETAILS

Gender:

[__] Male [__] Female

Age:

[__] Below 20 [__] 21-30 [__] 31-40 [__] 41-50 [__] 51-60 [__] Above 60

Highest education level:

[__] Primary School [__] Secondary School [__] Certificate College [__] Diploma College [__] University

B. BANKING INFORMATION

(i). Do you operate a bank account?

[__] YES [__] NO

(ii). If Yes to question B (i) above, what is type of the account do you operate?

[__] Savings account [__] Current account [__] Both

(iii). Do you use the ATM for financial/ banking transactions?

[__] YES [__] NO

(iv). How long have you used the ATM to access your account?

[__] < 6 months

[__] 6 months to ONE year

[__] ONE year to TWO years

[__] TWO years to THREE years

[__] THREE years to FOUR years

[__] More than FOUR years

(v). How often do you make ATM transactions?

[__] Daily-once

[__] Daily –Several times

[__] Weekly-Once

[__] Weekly-several times

[__] Monthly-once

[__] Monthly-several times

[__] Occasionally (less than once a month)

(vi). What type of transactions do you perform using the ATM?

[__] Cash Withdrawals

[__] Cash deposits

[__] Cheque deposits

[__] Balance enquiry

[__] Account statement request

[__] Bill payment

[__] Cheque book request

[__] Any other payment

(Specify)_____

(vii). <u>What is the current ATM authentication mechanisms used in your bank?</u>

[__] PIN & Magnetic stripe card

[__] PIN & smart card

[__] PIN/biometric/ATM card

[__] Biometric & ATM Card

(viii). <u>Do you find the mechanism used in your bank's ATM secure?</u>

[__] YES [__] NO [__] I don't Know

<u>DETERMINANTS</u>

PERFORMANCE EXPECTANCY

1. Biometric ATM authentication is very necessary for combating ATM fraud.
   [__] Strongly disagree [__] Disagree [__] Neutral [__] Agree [__] Strongly agree

2. Less time is spent in biometric ATMs than the current ATMs.

   [__] Strongly disagree [__] Disagree [__] Neutral [__] Agree [__] Strongly agree

EFFORT EXPECTANCY

3. A Biometric ATM is be easy to learn

[__] Strongly disagree [__] Disagree [__] Neutral [__] Agree [__] Strongly agree

4. A Biometric ATM is easy to use than the current implementations

[__] Strongly disagree [__] Disagree [__] Neutral [__] Agree [__] Strongly agree

5. The enrollment process for biometric authentication is simple and easy than the current implementations

[__] Strongly disagree [__] Disagree [__] Neutral [__] Agree [__] strongly agree

SOCIAL INFLUENCE

6. My parents, siblings and friends think Biometric Authentication at the ATMs is better than the current implementations.

[__] Strongly disagree [__] Disagree [__] Neutral [__] Agree [__] Strongly agree

7. Using Biometric Authentication at the ATM makes me feel better than those who do not use it.

[__] Strongly disagree [__] Disagree [__] Neutral [__] Agree [__] Strongly agree

FACILITATING CONDITIONS

8. Bank officials are available to offer help biometric ATM use when I need it

[__] Strongly disagree [__] Disagree [__] Neutral [__] Agree [__] strongly agree

9. I know how to use biometric ATM well

[__] Strongly disagree [__] Disagree [__] Neutral [__] Agree [__] Strongly agree

USER PRIVACY

10. I have privacy concern in the Biometric Authentication at the ATM

[__] Strongly disagree [__] Disagree [__] Neutral [__] Agree [__] Strongly agree

11. I feel that a third party may gain access to the biometric data.

[__] Strongly disagree [__] Disagree [__] Neutral [__] Agree [__] Strongly agree

BEHAVIORAL INTENTION

12. I intend to use Biometric Authentication at the ATM in the near future

[__] Strongly disagree [__] Disagree [__] Neutral [__] Agree [__] Strongly agree

13. I recommend financial service providers to adopt Biometric Authentication at the ATM

[__] Strongly disagree [__] Disagree [__] Neutral [__] Agree [__] Strongly agree

APPENDIX 3 Project Schedule

Task	Week1	Week2	Week3	Week4	Week5	Week6	Week7	Week8	Week9	Week10	Week11
Proposal Writing											
Proposal Presentation at faculty (Milestone 1)											
Main field Data Collection											
Corrections and Milestone 2 Presentation											
Data Coding, Analysis and Interpretation											
Report writing, Milestone 3 Presentation And submission											

Table 24: Project schedule

APPENDIX 4 Project Budget

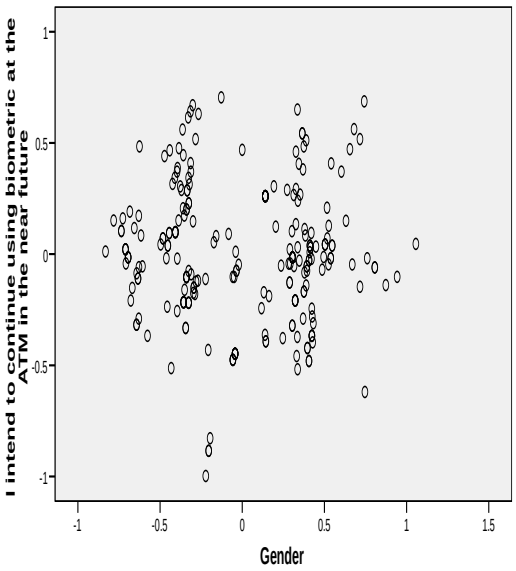
Activity	**Expenditure (Kshs)**
Data collection	30,000.00
Data analysis	15,000.00
Report preparation	5,000.00
Cost of Analysis of Moment Structures (AMOS) software.	40,000.00
Total	**90,000.00**

Table 25: Project Budget

APPENDIX 5: PARTIAL REGRESSION PLOTS

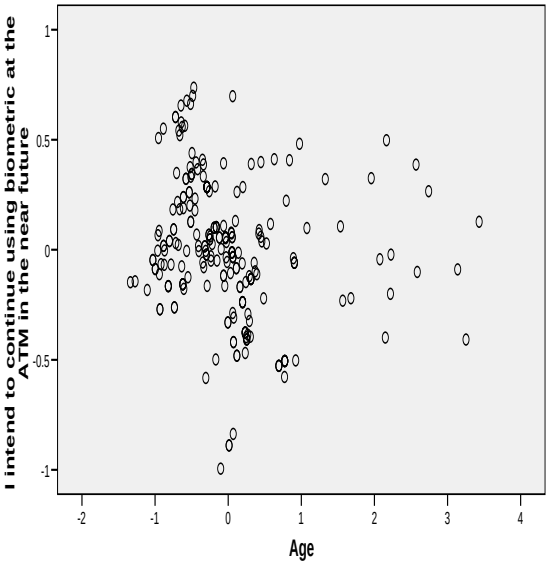
Partial Regression Plot

Dependent Variable: I intend to continue using biometric at the ATM in the near future



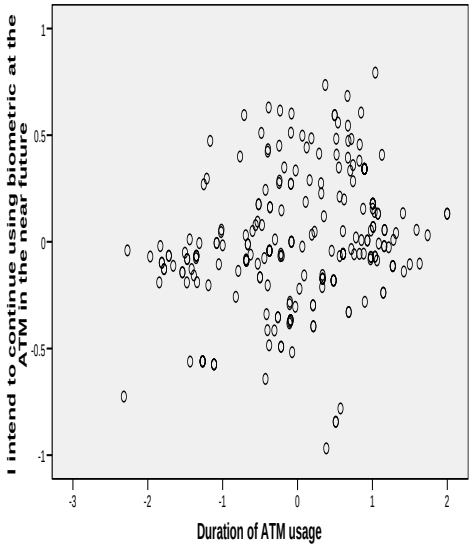
Partial Regression Plot

Dependent Variable: I intend to continue using biometric at the ATM in the near future



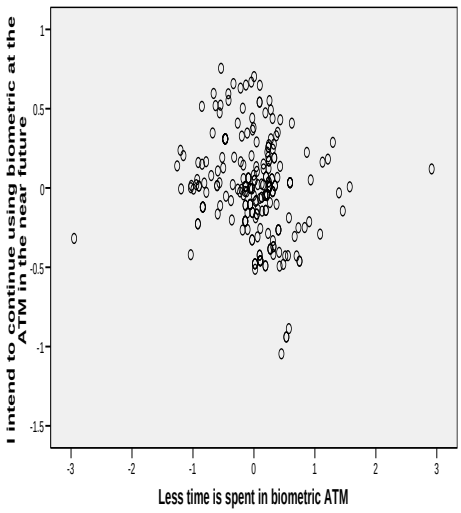
Partial Regression Plot

Dependent Variable: I intend to continue using biometric at the ATM in the near future



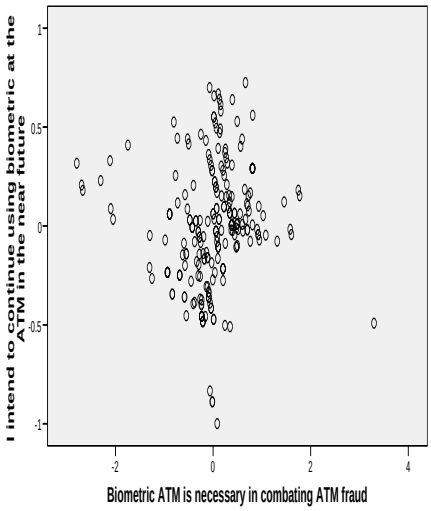
Partial Regression Plot

Dependent Variable: I intend to continue using biometric at the ATM in the near future



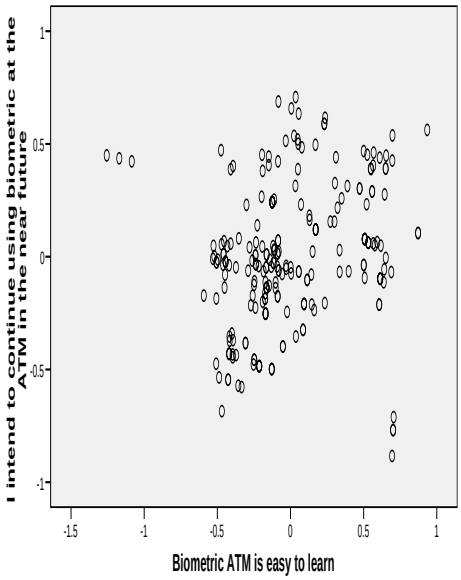
Partial Regression Plot

Dependent Variable: I intend to continue using biometric at the ATM in the near future



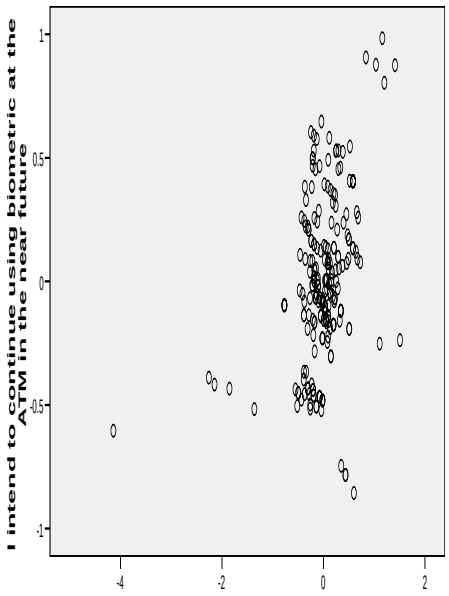
Partial Regression Plot

Dependent Variable: I intend to continue using biometric at the ATM in the near future



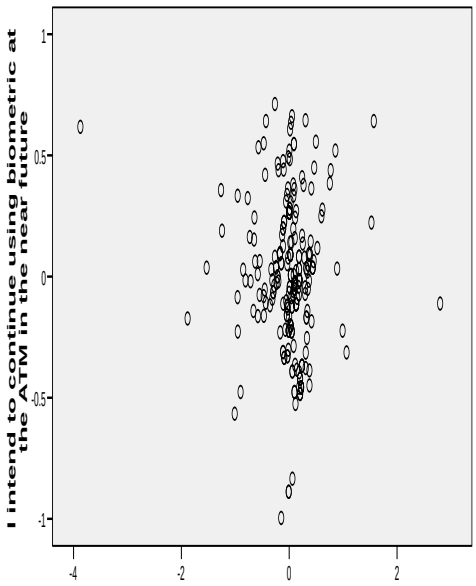
Partial Regression Plot

Dependent Variable: I intend to continue using biometric at the ATM in the near future



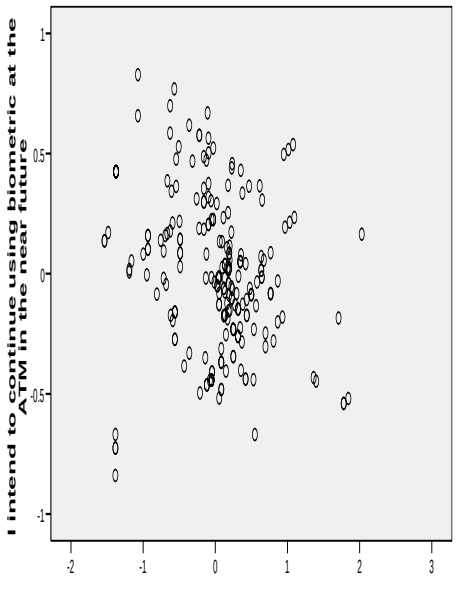
Partial Regression Plot

Dependent Variable: I intend to continue using biometric at the ATM in the near future



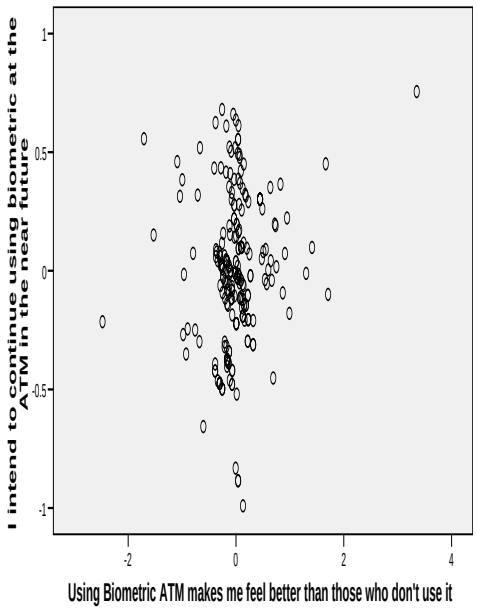
Partial Regression Plot

Dependent Variable: I intend to continue using biometric at the ATM in the near future

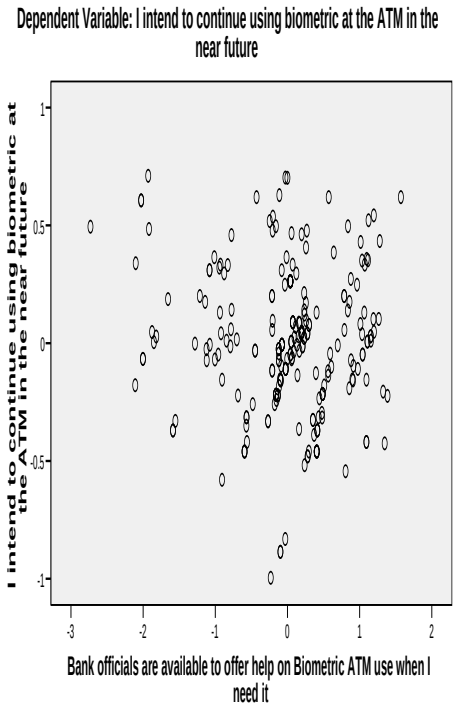


Partial Regression Plot

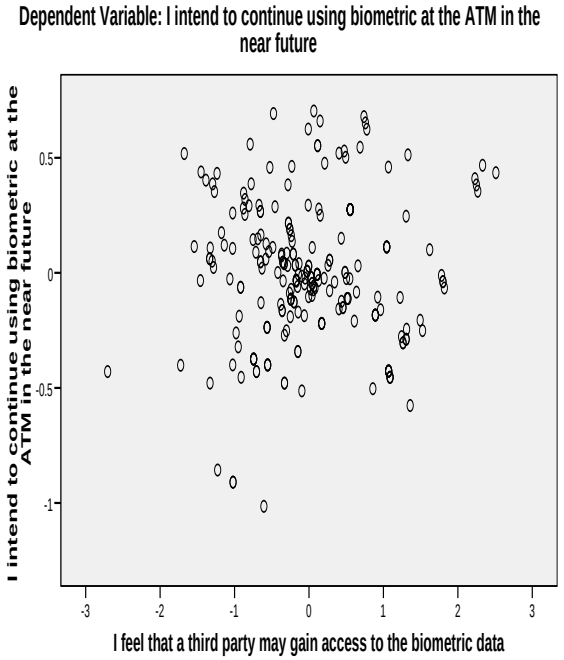
Dependent Variable: I intend to continue using biometric at the ATM in the near future



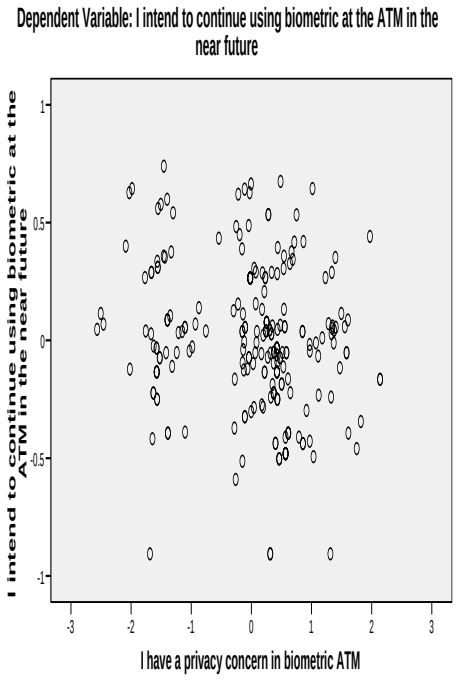
Partial Regression Plot



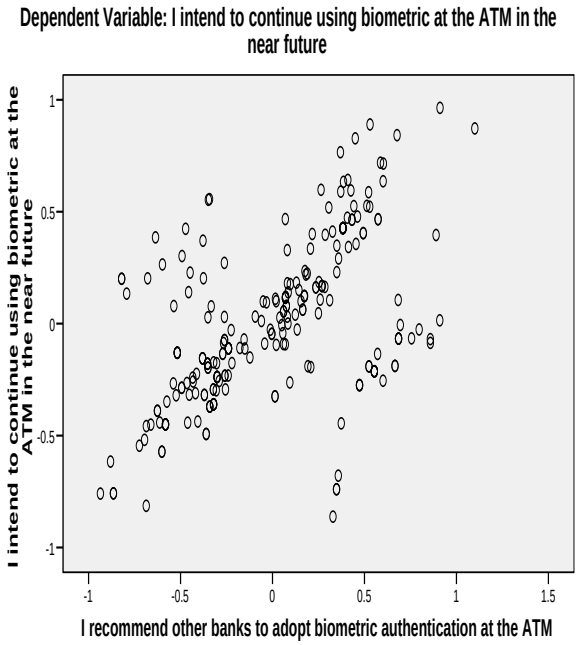
Partial Regression Plot



Partial Regression Plot

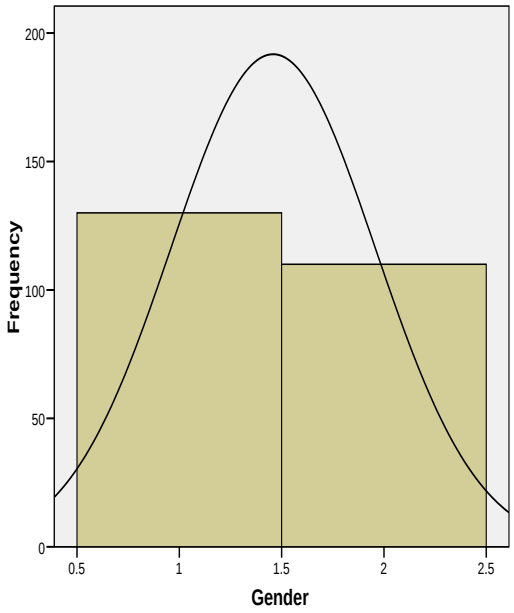


Partial Regression Plot

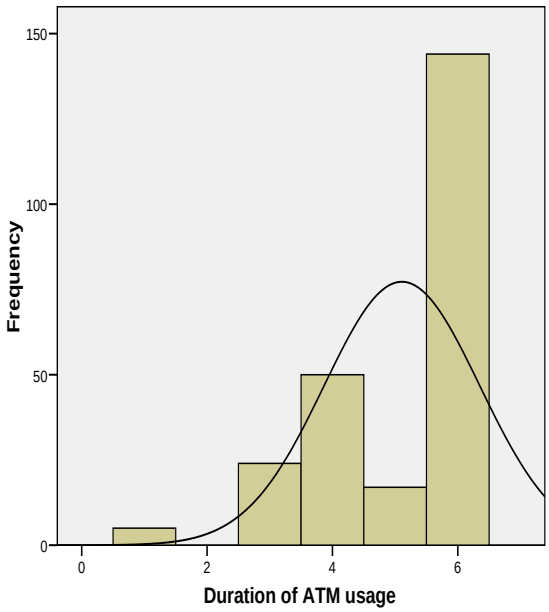


APPENDIX 6: HISTOGRAMS

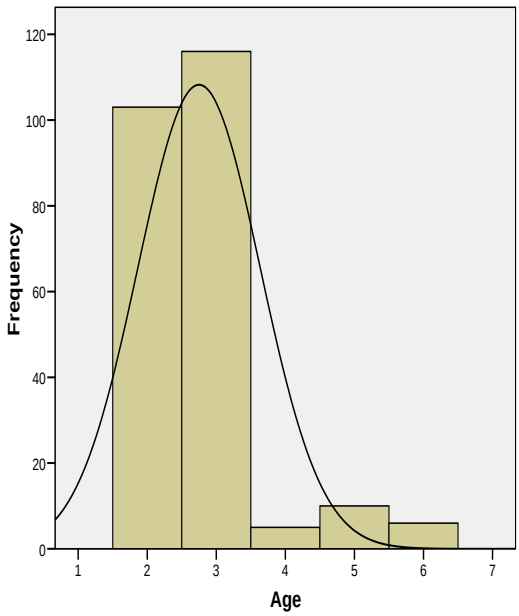
Gender



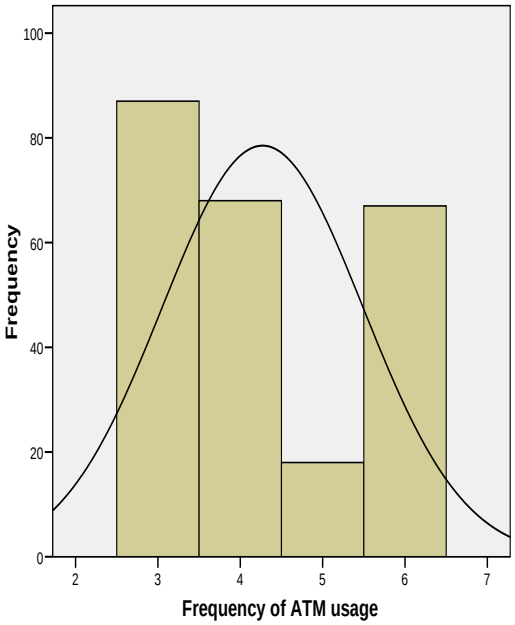
Duration of ATM usage

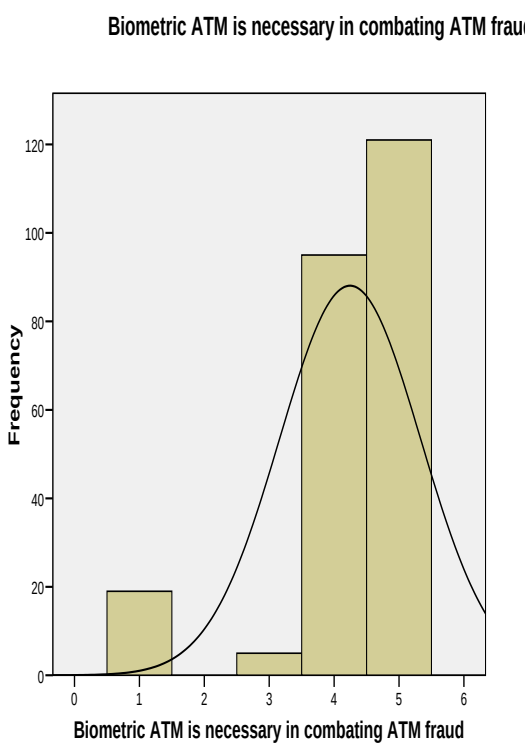


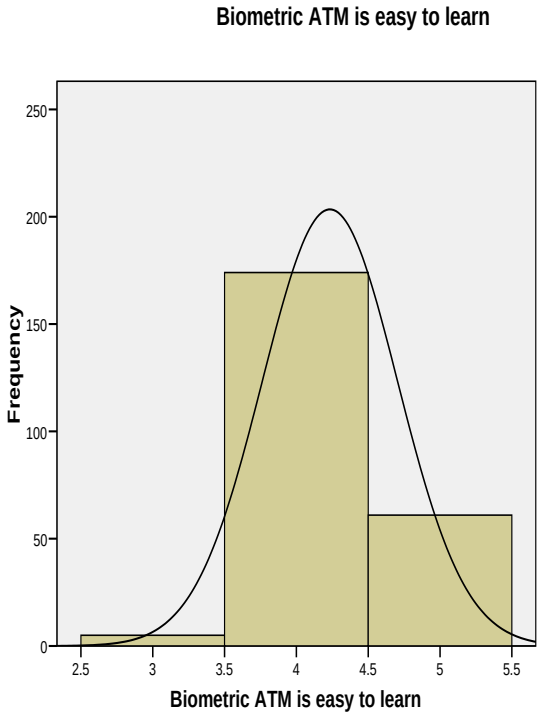
Age

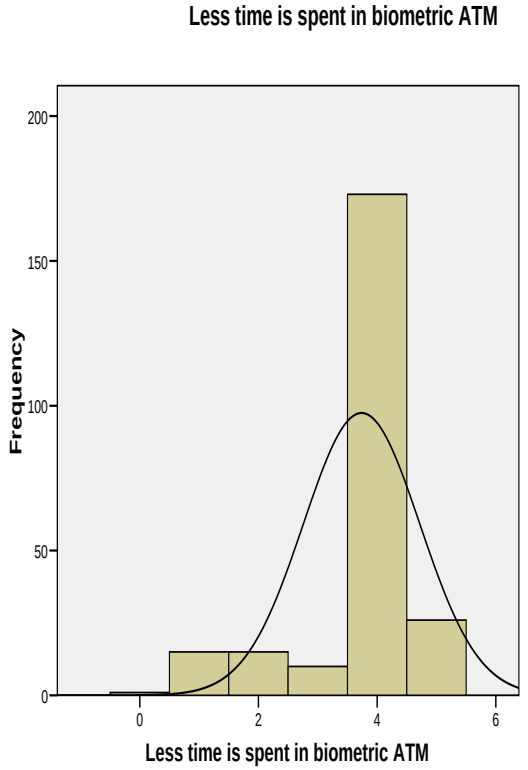


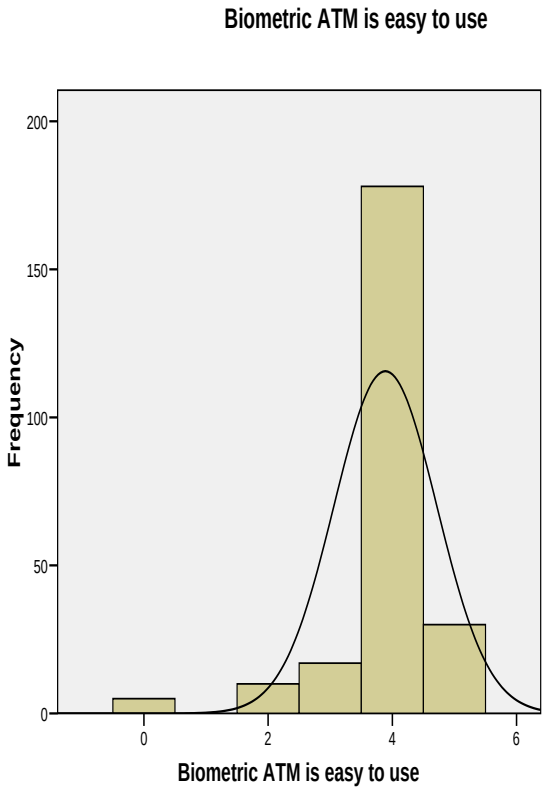
Frequency of ATM usage



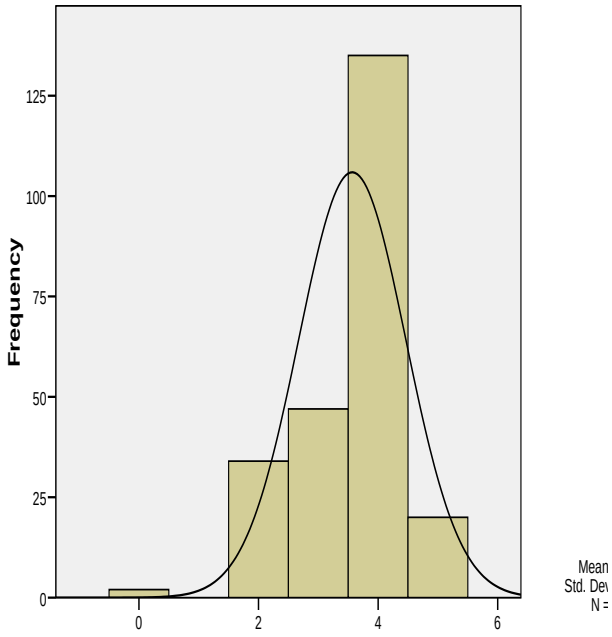

Biometric ATM is necessary in combating ATM frau
Frequency
120
100
80
60
40
20
0
0
1
2
3
4
5
6
Biometric ATM is necessary in combating ATM fraud


Biometric ATM is easy to learn
Frequency
250
200
150
100
50
0
2.5
3
3.5
4
4.5
5
5.5
Biometric ATM is easy to learn


Less time is spent in biometric ATM
Frequency
200
150
100
50
0
0
2
4
6
Less time is spent in biometric ATM

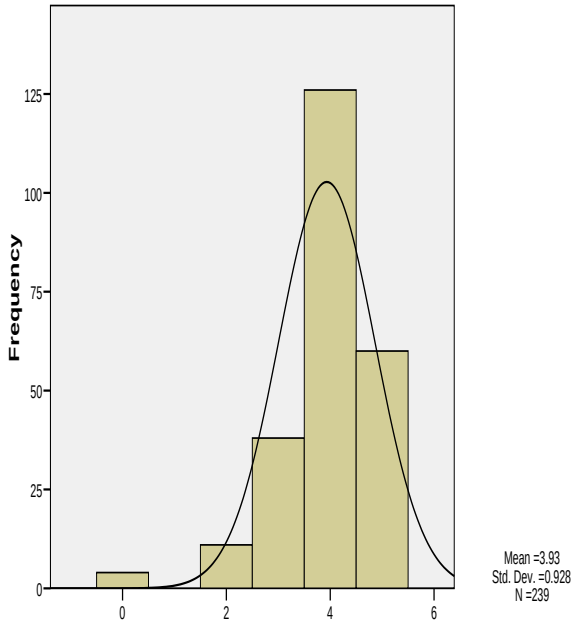

Biometric ATM is easy to use
Frequency
200
150
100
50
0
0
2
4
6
Biometric ATM is easy to use

The enrollment process for biometric authentication is simple and



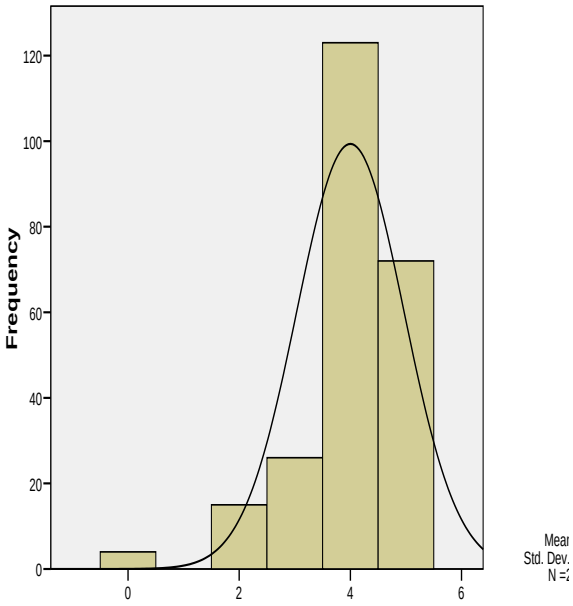
The enrollment process for biometric authentication is simple and easy

My parents,siblings,friends and other relatives think Biometric ATM is better than other authentications



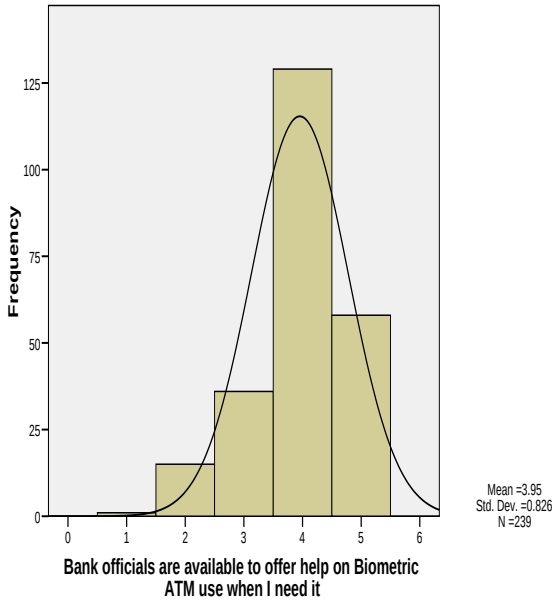
My parents,siblings,friends and other relatives think Biometric ATM is better than other authentications

Using Biometric ATM makes me feel better than those who don't u



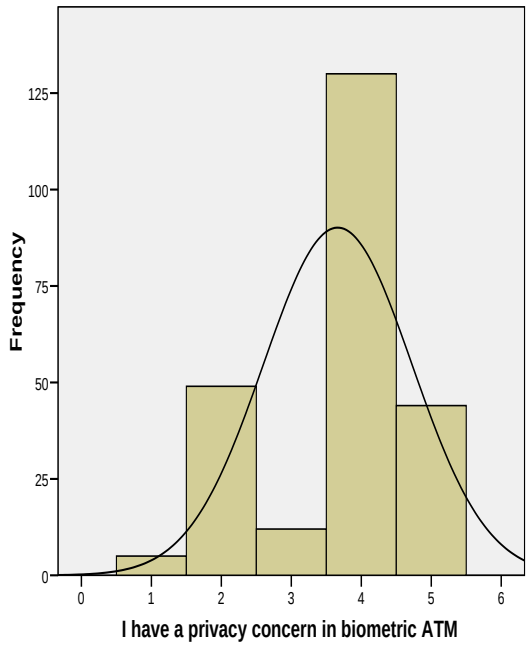
Using Biometric ATM makes me feel better than those who don't use it

Bank officials are available to offer help on Biometric ATM use when I need it

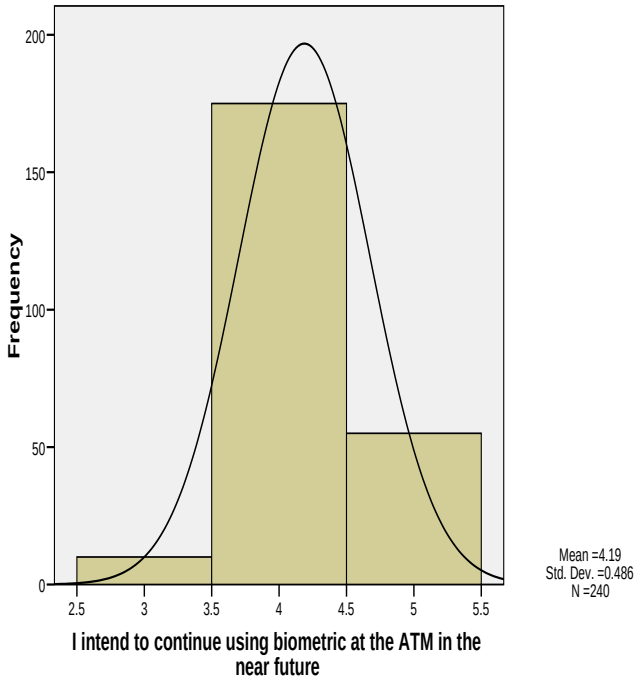


Bank officials are available to offer help on Biometric ATM use when I need it

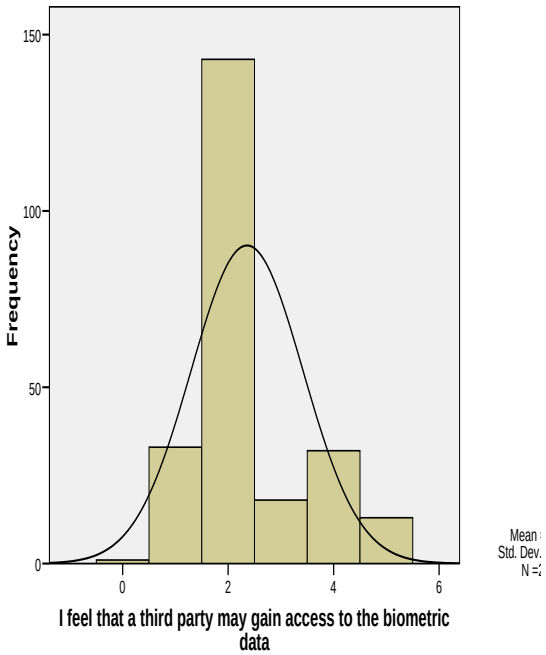
I have a privacy concern in biometric ATM



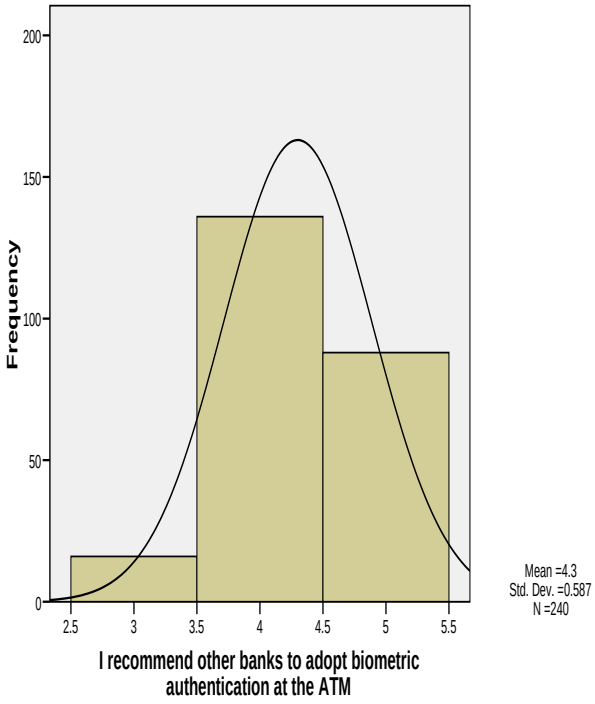
I intend to continue using biometric at the ATM in the near future



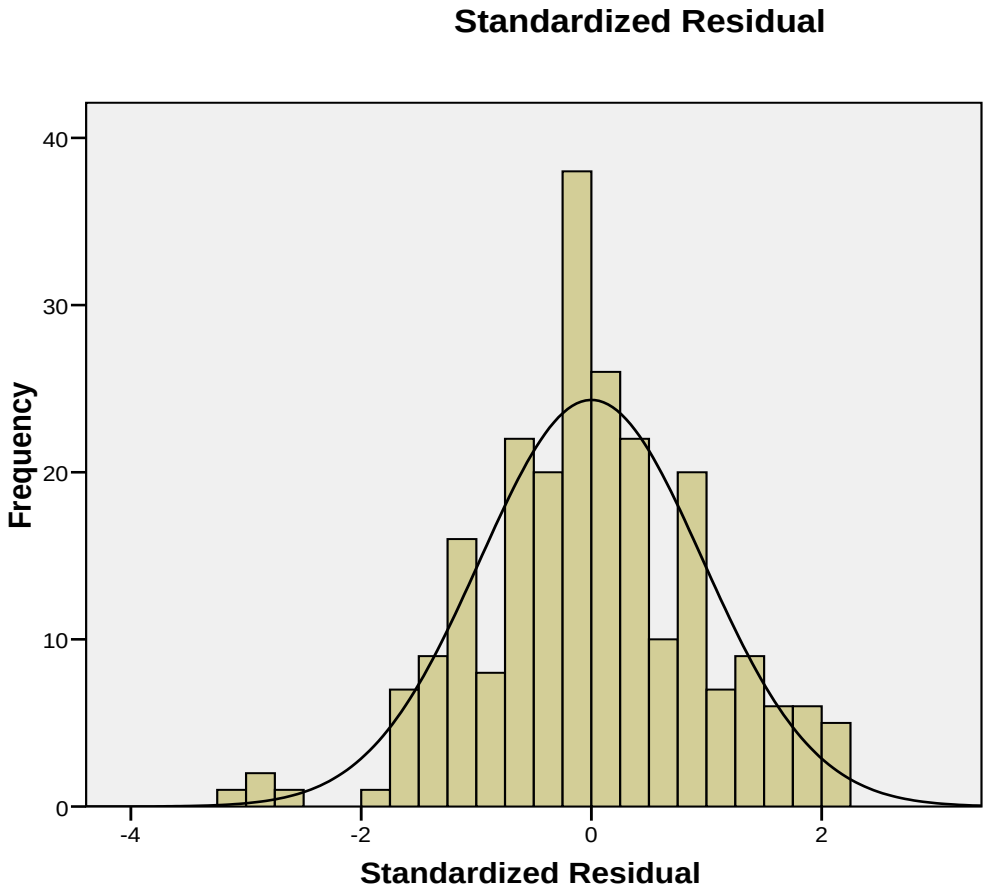
I feel that a third party may gain access to the biometric data



I recommend other banks to adopt biometric authentication at the ATM

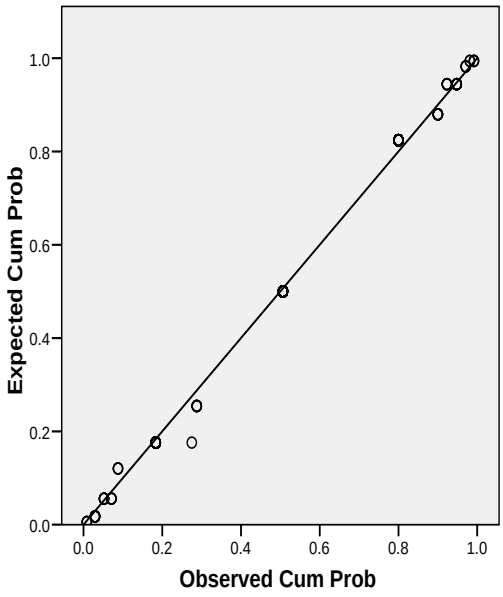


APPENDIX 7: STANDARDIZED RESIDUAL



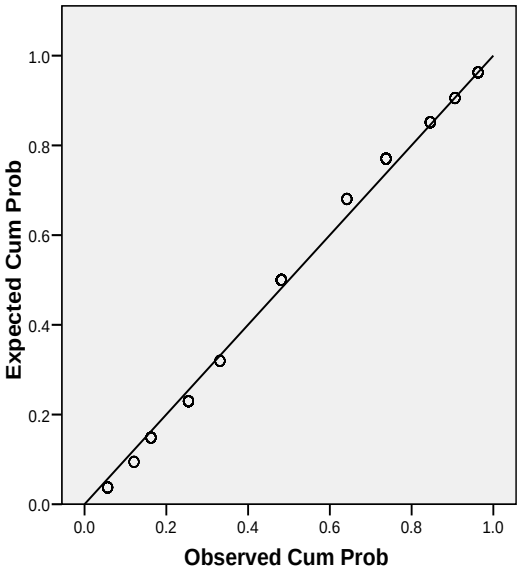
APPENDIX 8: P-P PLOTS

Normal P-P Plot of Age



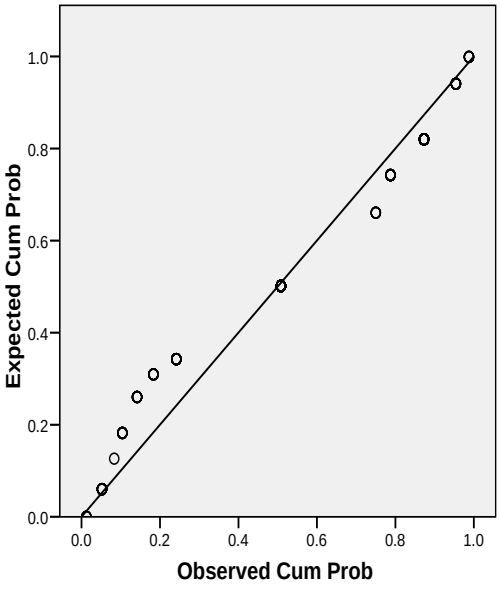
Transforms: natural log, difference(1)

Normal P-P Plot of Frequency of ATM usage



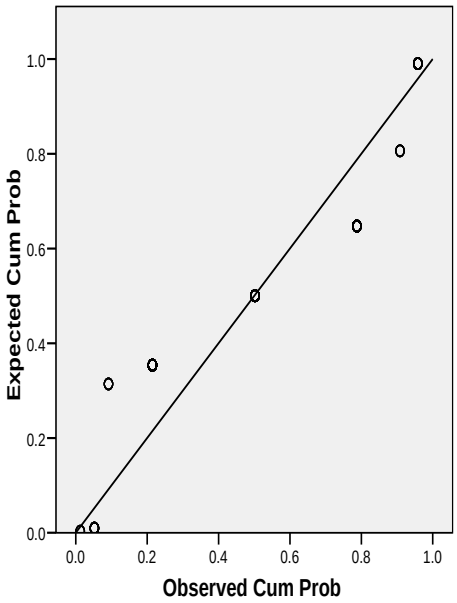
Transforms: natural log, difference(1)

Normal P-P Plot of Duration of ATM usage



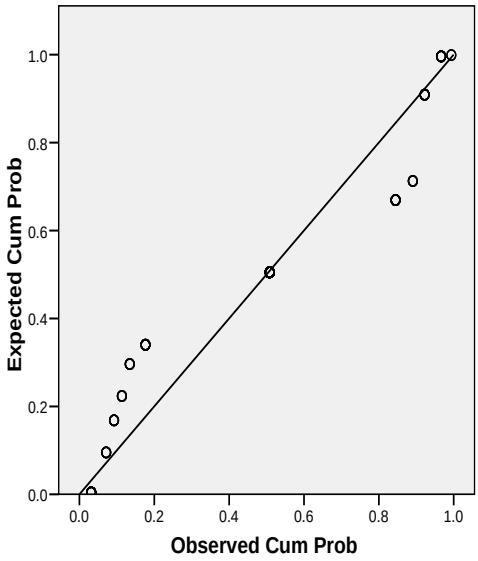
Transforms: natural log, difference(1)

Normal P-P Plot of Biometric ATM is necessary in combating ATM frau



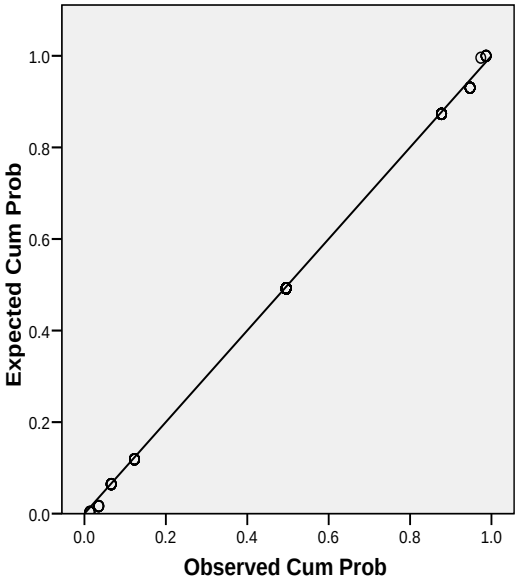
Transforms: natural log, difference(1)

Normal P-P Plot of Less time is spent in biometric ATM



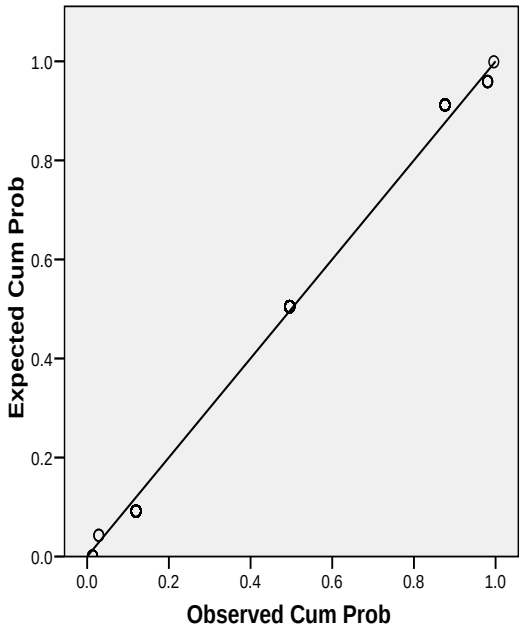
Transforms: natural log, difference(1)

Normal P-P Plot of Biometric ATM is easy to use



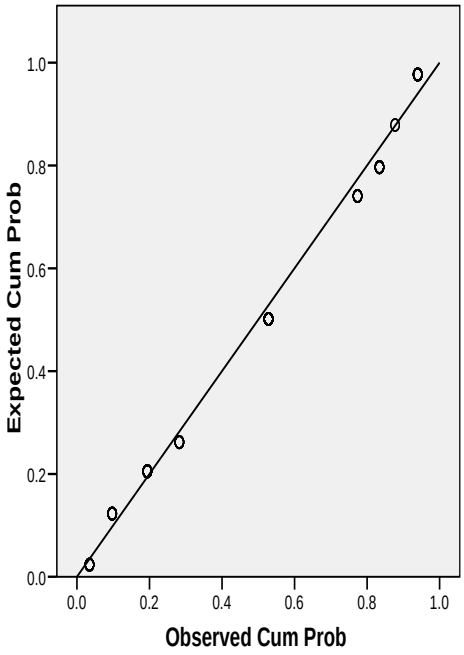
Transforms: natural log, difference(1)

Normal P-P Plot of Biometric ATM is easy to learn



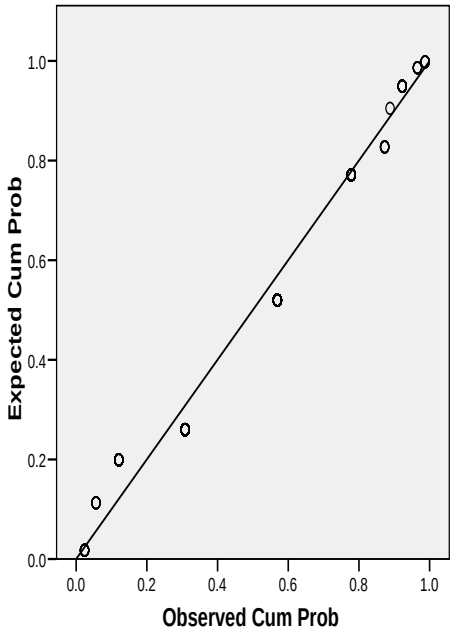
Transforms: natural log, difference(1)

Normal P-P Plot of The enrollment process for biometric authentication is simple and easy



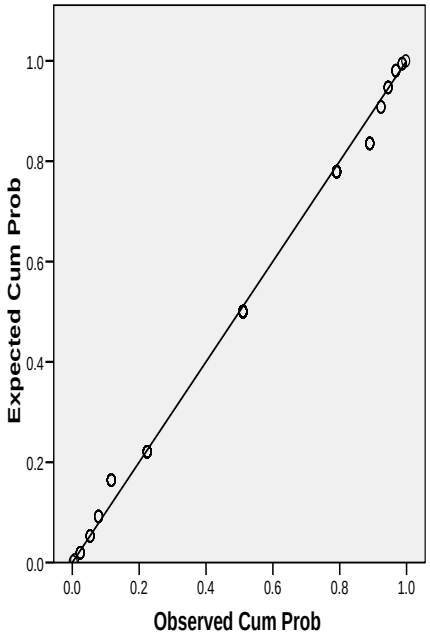
Transforms: natural log, difference(1)

Normal P-P Plot of Using Biometric ATM makes me feel better thar don't use it



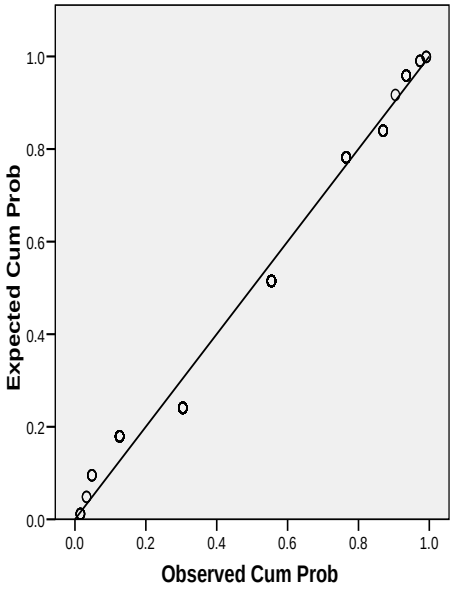
Transforms: natural log, difference(1)

Logistic P-P Plot of Bank officials are available to offer help on Biometric ATM use when I need it



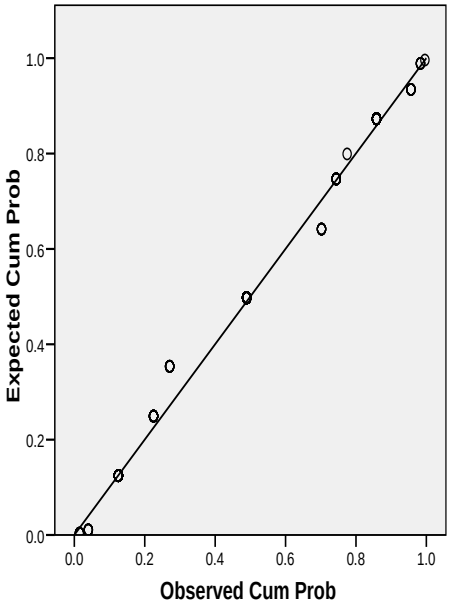
Transforms: natural log, difference(1)

Normal P-P Plot of My parents,siblings,friends and other relatives Biometric ATM is better than other authentications



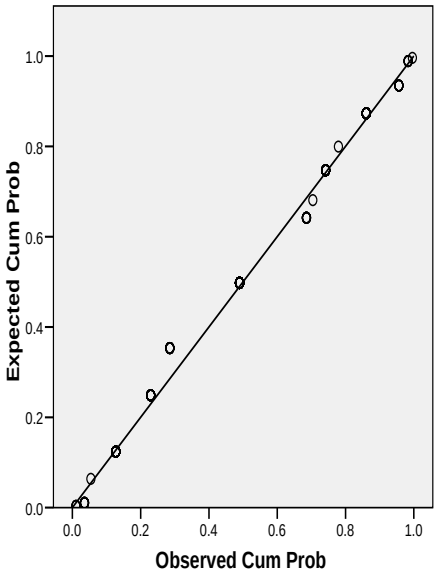
Transforms: natural log, difference(1)

Normal P-P Plot of I have a privacy concern in biometric ATM



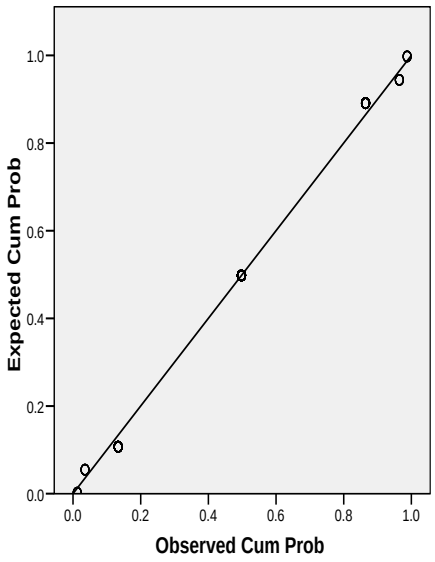
Transforms: natural log, difference(1)

Normal P-P Plot of I feel that a third party may gain access to the bion data



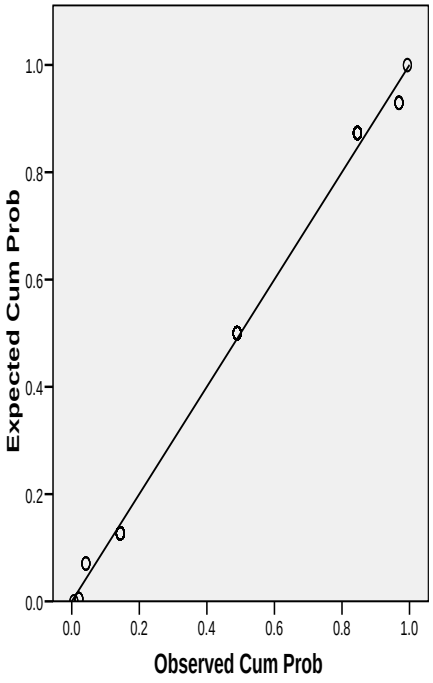
Transforms: natural log, difference(1)

Normal P-P Plot of I recommend banks to adopt biometric authentication at the ATM



Transforms: natural log, difference(1)

Normal P-P Plot of I intend to use biometric at the ATM in the near



Transforms: natural log, difference(1)