



Vaal University of Technology

Your world to a better future

USERS' PERCEPTIONS ON SECURITY OF MOBILE COMPUTING FOR ADOPTION OF E-APPLICATIONS IN SOUTH AFRICA

by

FHATUWANI VIVIAN MAPANDE

STUDENT NO: 207028028

Submitted in accordance with the requirements for the degree of

MAGISTER TECHNOLOGIAE

in the subject of

INFORMATION TECHNOLOGY

at the

VAAAL UNIVERSITY OF TECHNOLOGY

SUPERVISOR: PROF. TRANOS ZUVA

CO-SUPERVISOR: MR MARTIN APPIAH

DECLARATION

This thesis was written as a part of MTech in Information Technology at Vaal University of Technology. I declare that “Users’ perceptions on security of mobile computing for adoption of e-applications in South Africa” is my own work, that it has not been submitted for any degree or examination in any university, and that all the sources I have used or quoted have been indicated and acknowledged by complete references.

Full Names: Mapande Fhatuwani Vivian

Year: 2018

DEDICATION

This research report is dedicated to my daughter Reatlegile Uhone Manamela, my husband Sandile Manamela, my father Thomas Mapande, my mother Johannah Madilonga and my brother Tshifhiwa Mapande. Thank you for making me who I am today and the support you gave me.

ACKNOWLEDGEMENTS

Whilst I fully accept responsibility for the content presented in this research report, I am very much aware that it could not have been completed successfully without the cooperation of a number of people, who gave their moral support, intellectual expertise, experience, views and time.

Therefore, I will not do justice to myself, if I do not express my warm gratitude and appreciation to my supervisor Professor Tranos Zuva, whose professionalism, intellectual and significant guidance, support and suggestions helped me throughout this research effort. He availed himself at all times and has been patient with me until the study reached its logical conclusion.

To my co-supervisor Mr Martin Appiah, who availed himself at all times when I needed help and has been patient with me until the study reached its logical conclusion. To my husband Sandile Manamela, for all the support he gave me through those sleepless nights. To my brother Tshifhiwa Mapande, who has always been there for me with his inspiration and support. To you all, I say thank you for your valuable contributions.

Finally, I would like to thank all those people who availed their precious time during the data gathering process of this research report, without them this research wouldn't be a success.

ABSTRACT

The advancement of technology, particularly in the area of mobile computing, revolutionizes the way business is done in many industries such as the education sector, government sector, financial institutions, retail sector and the way people conduct their daily activities. The current technology provides influential tools for organisations and can significantly influence their operation, structure and approach. The development of mobile computing has created a new innovation for various industries by increasing the availability, frequency and speed of communication between the organisations and the individuals. However, users' perceptions can play an important role towards the adoption of these new developments.

The overriding purpose of this study was to investigate the users' perceptions on the security of mobile computing in South Africa for adoption of e-applications. The literature review was concentrated on the process of progressive development occurring during the study. To accomplish that goal it became necessary to reach some essential objectives i.e. investigating the users' perceptions models in literature. For the purpose of the study, it was important to propose a research framework for users' perceptions on the security of mobile computing with the potential for the adoption of e-applications in South Africa. The research evaluated the proposed framework to establish if there is any relationship between the e-application adoption factors. Furthermore, the hypotheses were tested to determine which factors would influence the adoption of e-applications in South Africa.

Technology Adoption Model 2 (TAM2) and Diffusion of Innovation (DOI) provide the theoretical basis for explaining how users perceive e-application services that they access and operate through mobile computing. To achieve that, a quantitative study was conducted with South African residents, with respect to mobile security perceptions; 476 valid questionnaires were received from the participants who were selected non-randomly. Questionnaires were developed from the proposed research framework derived from DOI and TAM2 and the items were adopted from other prior technology adoption studies. Through the use of the survey instrument developed for this study, data were collected in order to address the importance of this study based on the problem statement posed in the first chapter of this dissertation.

The valid questionnaires were analysed by using the Statistical Package for the Social Sciences (SPSS), Version 24.0. Reliability analysis, principal component analysis, correlations and multiple linear regression tests were conducted. Among other things this study made sure that

ethical considerations are adhered to. The findings revealed positive relationships between perceived usefulness of security mechanisms, perceived ease of use of security mechanisms, subjective norm on security mechanisms, relative advantage of security mechanisms, compatibility of security mechanisms, complexity of security mechanisms, aesthetics of security mechanisms interface and intention to adopt e-applications. Furthermore, subjective norm on security mechanisms was strongly correlated to intention to adopt e-applications, complexity of security mechanisms strongly correlated to perceived usefulness of security mechanisms, relative advantage of security mechanisms and aesthetic of security mechanisms interface strongly correlated to perceived usefulness of security mechanisms.

In addition, subjective norm of security mechanisms strongly influence intention to adopt e-applications in South Africa. Also, aesthetics of security mechanisms interface strongly influence both perceived usefulness of security mechanisms and perceived ease of use of security mechanisms. The reason behind it may be interpreted as users nowadays seeing the beauty as the platform to attract and encourage them to use e-applications. Finally, the proposed model analysis and survey evaluation will enable South African organizations to make informed decisions about the use of e-applications services. These findings contribute to a road map for the education sector, government sector, financial institutions, and retail sector as well as to encourage their customers or clients to adopt e-applications.

Keywords: *Adoption, security mechanism, e-applications, Diffusion of Innovation (DOI), Technology Adoption Model 2(TAM), Perceptions, Mobile computing*

TABLE OF CONTENTS

| | |
|---|-----|
| DECLARATION | ii |
| DEDICATION | iii |
| ACKNOWLEDGEMENTS | iv |
| ABSTRACT | v |
| LIST OF ABBREVIATIONS | x |
| LIST OF TABLES | xi |
| LIST OF FIGURES | xii |
| CHAPTER 1: INTRODUCTION | 1 |
| 1.1 PURPOSE OF THE STUDY | 1 |
| 1.2 STUDY BACKGROUND | 1 |
| 1.3 PROBLEM STATEMENT | 3 |
| 1.4 RESEARCH QUESTIONS | 4 |
| 1.5 RESEARCH OBJECTIVES | 5 |
| 1.6 SIGNIFICANCE OF THE STUDY | 5 |
| 1.7 DELIMITATIONS OF THE STUDY | 5 |
| 1.8 ASSUMPTIONS | 6 |
| 1.9 STRUCTURE OF THE THESIS | 6 |
| CHAPTER 2: LITERATURE REVIEW | 8 |
| 2.1 INTRODUCTION | 8 |
| 2.2 MOBILE COMPUTING | 8 |
| 2.3 SECURITY ISSUES IN MOBILE COMPUTING | 10 |
| 2.4 USERS AND MOBILE COMPUTING | 13 |
| 2.5 E-APPLICATIONS | 14 |
| 2.5.1 WHAT IS E-APPLICATIONS | 14 |
| 2.5.2 TYPES OF E-APPLICATIONS | 14 |

| | |
|---|----|
| 2.6 TECHNOLOGY ADOPTION MODELS | 36 |
| 2.6.1 THEORY OF REASONED ACTION (TRA) | 37 |
| 2.6.2 DIFFUSION OF INNOVATION THEORY (DOI) | 39 |
| 2.6.3 TECHNOLOGY ACCEPTANCE MODEL..... | 42 |
| 2.6.4 TECHNOLOGY ACCEPTANCE MODEL 2 (TAM 2) | 45 |
| 2.6.5 TECHNOLOGY ACCEPTANCE MODEL 3 (TAM3) | 46 |
| 2.6.6 THEORY OF PLANNED BEHAVIOUR (TPB) | 48 |
| 2.6.7 UNIFIED THEORY OF ACCEPTANCE AND USE OF TECHNOLOGY (UTAUT) | 49 |
| 2.6.8 TECHNOLOGY-ORGANIZATION-ENVIRONMENT MODEL (TOE) | 51 |
| 2.7 SUMMARY OF TECHNOLOGY ADOPTION MODELS | 54 |
| 2.8 CHAPTER 2 SUMMARY..... | 61 |
| CHAPTER 3: RESEARCH METHODOLOGY | 62 |
| 3.1 INTRODUCTION | 62 |
| 3.2 RESEARCH DESIGN | 62 |
| 3.2.1 THEORETICAL PHASE | 62 |
| 3.2.2 PORTRAYAL PHASE..... | 62 |
| 3.2.3 EXPLANATORY PHASE | 62 |
| 3.3 RESEARCH APPROACH | 63 |
| 3.4 POPULATION | 64 |
| 3.5 SAMPLING SIZE..... | 64 |
| 3.6 SAMPLING METHOD | 64 |
| 3.7 RESEARCH INSTRUMENT | 64 |
| 3.8 PROCEDURE FOR DATA COLLECTION | 66 |
| 3.8.1 VARIABLES AND OPERATIONAL DEFINITIONS..... | 70 |
| 3.8.2 PROPOSED RESEARCH MODEL..... | 71 |
| 3.9 ETHICAL CONSIDERATION | 72 |

| | |
|---|-----|
| 3.10 DATA PROCESSING AND ANALYSIS | 73 |
| 3.11 STUDY LIMITATIONS | 82 |
| 3.12 VALIDITY AND RELIABILITY | 82 |
| 3.12.1 VALIDITY | 82 |
| 3.12.2 RELIABILITY | 82 |
| 3.13 SUMMARY OF CHAPTER 3..... | 82 |
| CHAPTER 4: DATA PROCESSING AND ANALYSIS | 83 |
| 4.1 INTRODUCTION | 83 |
| 4.2 RESPONSE RATE | 83 |
| 4.3 RELIABILITY TEST RESULTS | 84 |
| 4.4 VALIDITY TEST RESULTS..... | 85 |
| 4.5 QUANTITATIVE ANALYSIS | 89 |
| 4.5.1 SECTION A: PARTICIPANTS' DEMOGRAPHIC INFORMATION..... | 89 |
| 4.5.2 SECTION B: USERS' PERCEPTIONS OF THE SECURITY OF MOBILE COMPUTING FOR ADOPTION OF E-APPLICATIONS | 92 |
| 4.6 RELATIONSHIPS BETWEEN THE VARIABLES | 113 |
| 4.7 HYPOTHESES TESTING RESULTS | 115 |
| 4.8 CONFIRMED RESEARCH MODEL..... | 118 |
| 4.9 CHAPTER SUMMARY..... | 119 |
| CHAPTER 5: CONCLUSION AND RECOMMENDATION | 121 |
| 5.1INTRODUCTION | 121 |
| 5.2 CONCLUSIONS..... | 121 |
| 5.3 RECOMMENDATIONS..... | 123 |
| 5.4 FUTURE WORK..... | 124 |
| APPENDIX A: INTRODUCTION LETTER..... | 147 |
| APPENDIX B: QUESTIONNAIRE..... | 148 |

LIST OF ABBREVIATIONS

| | |
|-------|--|
| PIN | Personal Identification Document |
| SPSS | Statistical Package for the Social Sciences |
| PDA | Personal Digital Assistant |
| GPS | Global Positioning System |
| B2C | Business to Consumer |
| PCS | Personal Communication Systems |
| OS | Operating System |
| FNB | First National Bank |
| ID | Identity Document |
| UCT | University of Cape Town |
| UJ | University of Johannesburg |
| SME | Small and Medium sized Enterprise |
| SMME | Small, Medium and Micro-sized Enterprise |
| WWW | World Wide Web |
| ICT | Information Communication Technology |
| SARS | South African Revenue Services |
| VAT | Value Added Tax |
| TAM | Technology Acceptance Model |
| TRA | Theory of Reasoned Action |
| DOI | Diffusion of Innovation |
| TPB | Theory of Planned Behaviour |
| UTAUT | Unified Theory of Acceptance and Use of Technology |
| TOE | Technology Organization Environment |
| PU | Perceived Usefulness |
| PEOU | Perceived Ease of Use |
| COMPL | Complexity |

| | |
|------|------------------------------|
| AEST | Aesthetics |
| SN | Subjective Norm |
| ITA | Intention to Adopt |
| COM | Compatibility |
| KMO | Kaiser-Meyer-Olkin |
| PCA | Principal Component Analysis |

LIST OF TABLES

| | |
|---|---------|
| Table 2.1: Technology Adoption Models Summary | 54 |
| Table 3.1: Survey questionnaire statements related to variables | 66 |
| Table 3.2: Study variables and operational definitions | 70 |
| Table 3.3: Reliability levels | 74 |
| Table 4.1: Reliability statistics for study constructs | 84 |
| Table 4.2: Sample adequate | 85 |
| Table 4.3: Eigenvalues-Total variance explained | 86 |
| Table 4.4: Factor loadings | 88 |
| Table 4.5: Users' demographic information | 91 |
| Table 4.6, 4.7, 4.8, & 4.9: Intention to adopt e-applications | 93-94 |
| Table 4.10, 4.11, 4.12, and 4.13: Perceived usefulness of security mechanisms | 95-97 |
| Table 4.14, 4.15, 4.16, and 4.17: Perceived ease of use of security mechanisms | 98-100 |
| Table 4.18, 4.19, 4.20, and 4.21: Aesthetics of security mechanisms interface | 101-103 |
| Table 4.22, 4.23, 4.24, and 4.25: Relative advantage of security mechanisms | 104-106 |

| | |
|--|---------|
| Table 4.26, 4.27, and 4.28: Subjective norm on security mechanisms | 107-108 |
| Table 4.29, 4.30, and 4.31: Compatibility of security mechanisms | 109-110 |
| Table 4.32, 4.33, 4.34, and 4.35: Complexity of security mechanisms | 111-113 |
| Table 4.36: Correlation Coefficient | 114 |
| Table 4.37: Hypotheses test results | 117 |

LIST OF FIGURES

| | |
|---|----|
| Figure 1.1: Outline of the study | 7 |
| Figure 2.1: Mobile computing | 10 |
| Figure 2.2: ABSA bank login screen | 18 |
| Figure 2.3: Nedbank login screen | 18 |
| Figure 2.4: Standard bank login screen | 18 |
| Figure 2.5: Capitec bank login screen | 18 |
| Figure 2.6: FNB bank login screen | 19 |
| Figure 2.7: Wits-e security interface | 25 |
| Figure 2.8: Sun-learn security interface | 25 |
| Figure 2.9: Vula security interface | 25 |
| Figure 2.10: Moodle/Learn security interface | 25 |
| Figure 2.11: Ulink security interface | 25 |
| Figure 2.12: The something you know Authentication mechanism | 30 |
| Figure 2.13: KAPAS security interface | 30 |
| Figure 2.14: YuppieChef security interface | 30 |

| | |
|--|-----|
| Figure 2.15: Bid or Buy security interface | 31 |
| Figure 2.16: Action Gear security interface | 31 |
| Figure 2.17: Takealot security interface | 31 |
| Figure 2.18: E-toll security interface | 35 |
| Figure 2.19: E-filing security interface | 35 |
| Figure 2.20: E-home affairs security interface | 36 |
| Figure 2.21: UFiling security interface | 36 |
| Figure 2.22: Theory of Reasoned Action Model | 39 |
| Figure 2.23: Diffusion of Innovation Model | 42 |
| Figure 2.24: Technology Acceptance Model (TAM) | 44 |
| Figure 2.25: Technology Acceptance Model 2 (TAM 2) | 46 |
| Figure 2.26: Technology Acceptance Model 2 (TAM 3) | 47 |
| Figure 2.27: Theory of Planned Behaviour Model | 48 |
| Figure 2.28: Unified Theory of Acceptance and use of Technology (UTAUT) | 51 |
| Figure 2.29: Technology Organization Environment Model (TOE) | 53 |
| Figure 3.1: Proposed research Model | 72 |
| Figure 3.2: Relationships between the users' perceptions on the security of mobile computing for adoption of e-applications | 77 |
| Figure 3.3: Study hypotheses | 78 |
| Figure 4.1: Correlation Coefficient | 115 |
| Figure 4.2: Confirmed proposed research Model | 119 |

CHAPTER 1: INTRODUCTION

1.1PURPOSE OF THE STUDY

The purpose of this study was to investigate users' perceptions on security of mobile computing for adoption of e-applications in South Africa.

1.2 STUDY BACKGROUND

Due to rapid development of interconnected online information technology infrastructure, users can access a wide range of online content and services. Many organisations and businesses such as the government sector, financial institutions, education sector and retail sector around the world have taken advantage of this innovation and were urged to keep up with this development to provide users with easy access to their products and services anywhere, anytime. These services and products fall under e-applications that include e-banking, e-commerce, e-learning, e-health and e-government. With the network being 99.9% digital and including the latest in fixed line, wireless and satellite communication, South Africa holds the most enlarged telecoms network in Africa (BusinessTech, 2017). South Africa has the fourth fastest growing mobile communication market in the world.

According to Kemp (2017) the population of South Africa is approximately 55.21 million based on 2017 estimates. The country has 28.66 million internet users with 52% penetration rate, where 92% of the population use mobile phones. Kemp (2017) further indicates that 69% use smartphones, 20% use laptops and 10% use tablets. According to the 2017 South Africa mobile report, 70% of the population browsed the internet through their mobile devices (Effectivemeasure, 2017). It was found that 21% of the South African population use smartphones to access mobile applications (Effectivemeasure, 2017). In addition, Vancouver (2017) has found that 34% of the South African population are using m-banking and 15% conduct purchases through e-commerce using mobile devices. This is as a result of the numerous advantages of accessing e-applications anytime, anywhere.

Regardless of these advantages, the use of mobile computing in South Africa is found to be low compared to other countries such as Spain, Singapore, Italy, Japan and South Korea (Kemp, 2017). In addition, Musaev and Yousoof (2015) state that when it comes to online information technology infrastructure, online security is a major concern. A number of studies

found security to be a major concern for users conducting online activities such as banking and purchases (Wei, Li, Cao, Ou & Chen, 2013). Achieving total security is impossible, as security is a moving target. According to Onwuzurike and De Cristofaro (2015) there are noticeable advances in developing security technologies that enhance the functional aspects of a security so as to moderate the ever-increasing trending threats that prevail in today's mobile computing environment. Leukfeldt, Kleemans and Stol (2016) affirm that the main challenge is getting the users to accept and embed their behaviour in a real security culture where they take responsibility and show accountability. This task is extremely challenging and nearly impossible, since human behaviour cannot be predicted or guaranteed.

Musaev and Yousoof (2015) mention that since e-applications provide internet based services, they should have secure and reliable methods of authenticating users. Therefore, e-application providers have to understand users, current adoption of e-applications and act quickly to market developments by identifying reasons that impact users' perceptions of security and usability issues in e-applications. (Teh, Zhang, Teoh & Chen, 2016) and Kiljan (2017) indicate that security and usability can be different. The reason being is that, if the user is required to perform security actions in addition to functional actions, it inherently decreases the usability of the system since the user has to perform more actions than what is strictly necessary to fulfil the users' goal or job. Usable security is more than just a link of the different terms usability and security. For this study, the term usable security refers to the usability of security interface with various security mechanisms (Abdulwahid, Clarke, Stengel, Furnell & Reich, 2015).

According to Leukfeldt, Kleemans and Stol (2016) user identification is a required ability of a multi-user system. Through user identification the system determines which functions and data are available to whom. Providing a username or some sort of identification that is associated with the user, such as Password/PIN, bank account or email address would be a functional action, since it is required to notify the system to know who is currently using it. Holz and Bentley (2016) support that by only asking for a username, the system is fully balanced towards usability. A security action can be introduced to ensure that users do not get access to functionality that is not assigned or meant for them.

According to Ur, Bees, Segreti, Bauer, Christin and Cranor (2016), a common illustration is the requirement to provide a password/PIN from a functional view; in this case the user is required to perform additional actions and spend more effort for the same outcome as when no password would be required. Password sharing or storing is often discouraged; users are

therefore expected to remember their passwords. Furthermore, Anwar and Brusilovsky (2017) affirm that introducing the security action disadvantaged some usability for security since the user is required to perform more work in order to use the system. A security action would cause this to happen to a certain degree if it involves the user and security actions such as multi-factor authentication, and biometric authentication.

1.3 PROBLEM STATEMENT

The software design of applications can go a long way in determining the usability and compatibility of those applications. Crawford, Renaud & Storer (2013) highlight the importance of integrating security and usability with the requirements and design processes. Prior studies (Halaweh, (2014), Damasevicius, Maskeliunas & Yenckauskas (2016), Alhussain, Alghamdi, Alkhalaf & Alfarraj, 2013) have since shown noticeable gains in shaping human behaviour through training and education. The conclusion can be complemented by taking the behaviour of users and perceptions of users into account when designing and developing security systems and interfaces.

The internet has become one of the most important channels providing anytime, anywhere online services and products to various people of different levels of knowledge. To promote the construction of life-long convenient, secure, usability and compatible e-applications, design which includes aesthetics and quality play a major role in security applications, where security is not the primary production task (Koved, Trewin, Swart, Singh, Cheng & Chari, 2013). The lack of results with regard to consideration of users' perceptions on security pertaining to aesthetics on security mechanisms, perceived usefulness and perceived ease of use of security mechanisms in South African communities, drives the need for research in this field.

In addition, Sun and Bin (2015) state that currently the internet and mobile devices are trending and innovations have threatened security considerations through time. Therefore, users tend to have a lack of understanding on how mobile computing applications and its security work. However, hackers have become smarter and users have become more mobile (Yao, Verima, Kang & Sezer, 2017). Halaweh (2014) studied users' perception of security for mobile communication technology. Halaweh (2014) further explored the users' perception of security towards mobile phones from a wide perspective. The results provided evidence for extending the meaning of the security perception concept to include human security as a relevant issue to mobile phone usage.

The results also showed that the development of mobile technology raises new security and privacy issues. Dai (2015) states that most researchers indicate that the current authentication method for the security of mobile devices depends on the use of a personal identification number (PIN) to verify users, although the use of a correct PIN doesn't guarantee a person's identity. This research is a work in progress. It looks at various aspects (identified from different research areas) of achieving the ultimate goal of designing usable security systems that users can embrace. It involves taking into account interface design, users' perceptions on security of mobile computing for adoption of e-applications. This will help to reduce the tendency of users doubting and bypassing security merely because of the effort needed to comply with security mechanisms.

Mwiya et al. (2017) highlight that there have been many studies on the technology adoption model in relation to factors influencing e-banking adoption; few have actually incorporated the element of trustworthiness of e-banking systems in terms of security, credibility and safety perceptions. Shatat (2017) mentions that the limitation of a study to a specific location helps to get a better understanding of the end-users' perceptions towards the online services and improves the representation of a population. The questionnaire should be conducted in various countries or locations in order to cover large sample sizes and get more respondents from different backgrounds and different environments. This study examines the users' perceptions on the security mechanisms. It also sought to discover the factors that influence the perceived usefulness of security mechanisms and perceived ease of use of security mechanisms.

1.4 RESEARCH QUESTIONS

This study is a continuation of other research work that has been conducted in South Africa that is not limited to users' perceptions on security of mobile computing for adoption of e-applications. Therefore, the following research questions are formulated as follows:

Research Question 1: What are the users' perceptions models for technology adoption?

Research Question 2: What are the relevant factors for users' perceptions on security of mobile computing for adoption of e-applications in South Africa?

Research Question 3: To what extent does the technology adoption factors correlate and influence on each other?

1.5 RESEARCH OBJECTIVES

The research objectives of this study have been formulated as follows:

- (i) To investigate users' perceptions models for technology adoption in literature
- (ii) To propose a framework for users' perceptions on security of mobile computing for adoption of e-applications in South Africa
- (iii) To evaluate the proposed framework

1.6 SIGNIFICANCE OF THE STUDY

The internet has brought about revolution, changing organisations and businesses' interaction with customers. According to ICASA (2016), the South African internet user population passed the 20 million mark for the first time in 2016. Now South Africa has 21 million internet users, mostly on mobile devices. The report also revealed that the most common use of the internet among South African adults is for communication. Therefore this study will be of great importance for these individuals to know and understand the perceived usefulness and perceived ease of use of security mechanisms while using the mobile devices.

Moreover, the findings of this study will contribute to the research literature of mobile computing technologies. This study attempts to add to the body of literature on the role of technology adoption studies in South Africa. Furthermore, the study will contribute theoretically in the area of security perceptions in adoption of e-applications. The field work of this study has produced sufficient evidence of the importance of perceived usefulness and perceived ease of use of security mechanisms considering it is playing an important role in the adoption of e-applications. This study is significant because it has provided comprehensive users' perceptions on security of mobile computing for the adoption of e-applications in South Africa.

1.7 DELIMITATIONS OF THE STUDY

The research was conducted in South Africa, targeting users with access to mobile devices. The survey was conducted on various online platforms such as Facebook and emails. Questionnaires were distributed via a link to ordinary email holders and also Facebook pages, and made public. The research covered the following main constructs of users' intention to adopt e-applications: perceived usefulness and ease of use of security mechanisms, aesthetics

of security mechanisms interface, relative advantage of security mechanisms, compatibility of security mechanisms, complexity of security mechanisms and subjective norm on security mechanisms. The research is based on technology adoption constructs derived from Diffusion of Innovation formulated by Rogers (2003) and Technology Adoption Model 2 proposed by Venkatesh and Davis (2000).

1.8 ASSUMPTIONS

The following assumptions have been made regarding the study:

- The total number of respondents was sufficient to gain adequate data
- Participants truthfully and honestly responded to the questionnaire

1.9 STRUCTURE OF THE THESIS

This Thesis consists of five chapters (Figure 1.1). Chapter 1 is already presented (see page 1-6). Chapter 2 presents the review of literature on various e-application types and the research conducted in the field of technology adoption models. The chapter provides a brief overview of the research backgrounds and the relationships between different terms.

Chapter 3 focuses on the research design, research approach, population, sampling size, sampling method, research instrument, procedure for data collection, proposed research model as well as presenting the hypothesis to be tested, ethical considerations, data processing and analysis, validity and reliability.

The data processing and analysis of the study is presented in chapter 4. The results are composed and examined using an appropriate tool, i.e. the Statistical Package for the Social Sciences (SPSS). The results are presented in figure and tabular forms. Comparison is done between the questionnaire groups. The research findings are integrated with the results from the related research in the literature review.

The study findings are summarized in Chapter 5. Furthermore, chapter 5 focuses on answering the research questions and presenting recommendations for considering users' perceptions on security of mobile computing for adoption of e-applications in South Africa.

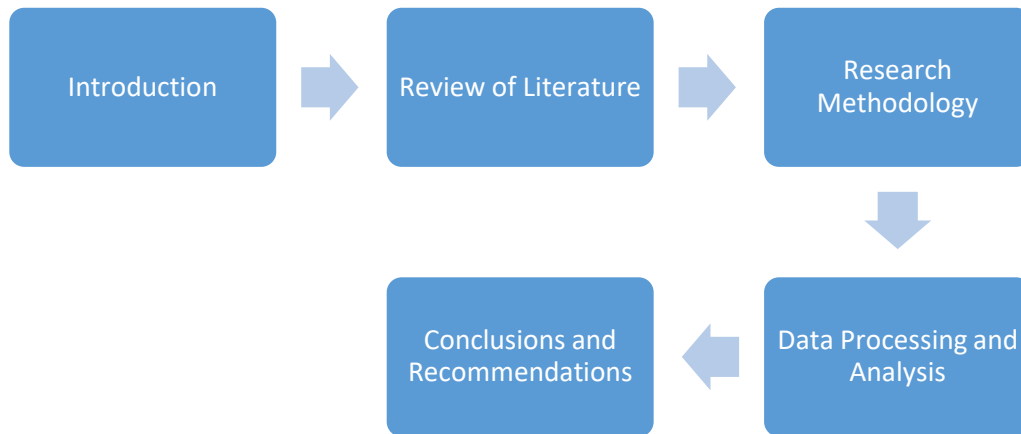


Figure 1.1: Outline of the study

CHAPTER 2: LITERATURE REVIEW

2.1 INTRODUCTION

The literature review will assist the reader to become familiar with the basic terminologies used in this study, i.e. mobile computing, e-applications and its aspects. This chapter covers mobile computing security, types of e-applications, e-applications security issues, users' perceptions in South Africa, technology adoption models and the comparison of different technology adoption models.

2.2 MOBILE COMPUTING

According to Rajan and Jayashree (2015), mobile computing is a variety of wireless devices such as tablets, smart phones, and laptops that have the ability to allow people to connect to the internet and has increased user dependence on the internet for communication and transactions. Krishna and Muniyal (2015) substantiate that mobile computing provides flexibility of the computing environment over physical mobility. The user of a mobile computing environment will be able to access data, information or other logical objects from any device in any network while on the move, although various researchers have written about security issues, privacy and challenging features concerning mobile computing.

The first computing, namely abacus, was used in 500 B.C. which may be considered as mobile computing, because abacus is small in size, it can be portable, and the calculating numbers are one part of computing (Alotaibi & Albar, 2016). The concept of networks (both wired and wireless) appeared between the years 1960-1970. In 1970-1980, it was the emergence and use of satellite, and then followed by the use of cellular technologies in the period of 1980-2000.

Mobile computing has signalled a new era in the field of computing and information systems. The concept of mobile computing is derived from the realization that as computing machinery decrease in size and increase in computing power, users will demand these machineries to be part of their everyday life (Balwir & Kondekar, 2015). Mobile computing has also been seen as a mixture of moveable computers, modems and telephone network (Patil & Gaikwad, 2015).

Most research (Alwan & Al-Zu'bi (2016), Shatat (2017)) has found that mobile computing is subject to security and privacy risks. Mobile computing tends to and is able to collect more personal data from users (Dai, 2015). With mobile computing the need to be impounded within one physical location has been eliminated. The introduction of portable computers and laptops,

Personal Digital Assistants (PDAs), smart phones and tablets has in turn made mobile computing very convenient. The essence of mobile computing is to be able to work from any location (Shin, Lee & Odom, 2014).

According to Paul and Sharma (2014), mobile computing is associated with the ability to use hardware, data and software in computer applications for communication. The study of this new era of computing has prompted the need to rethink carefully about the way in which mobile network and systems are conceived. Even though mobile and traditional distributed systems may appear to be closely related, there are a number of factors that differentiate mobile and traditional distributed systems, especially in terms of type of device (fixed/ mobile), network connection (permanent/ intermittent) and execution context (static/dynamic).

Due to leading companies such as Amazon, Google, Apple and Microsoft, developing innovative mobile devices, smart wearable devices are the next mobile computing devices with great market potential (Weng & Lin, 2015). Mobile computing offers users mobility to connect to the internet anywhere and anytime. It also provides the ability to bring mobile communication to remote areas at lower cost without any pre-existing communication. Mobile computing provides applications such as cloud computing (Mohamed, Hamed & Bader, 2015). Sanaei, Abolfazli, Gani and Buyya (2014) define mobile computing as the design of small, powerful devices such as smartphones, personal digital assistant (PDA), wearable computers, global positioning systems (GPS) and laptops that enable mobility in wireless networks which supports a trend toward computing on the go, with the help of wireless technology like wimax, Ad Hoc network and Wifi. Suganya and Shanthi (2015) describe the vision of mobile computing as “information at fingertips anywhere, anytime”.

According to Tahir (2013), one challenge in mobile computing is to make use of the changing environment with a new group of applications that are conscious of the context in which they run. Tahir (2013) went on by saying that mobile computing environment is distributive, where we have mobile hardware (mobile devices) as clients have mobile software in them and information systems such as internet, satellites etc. as servers. Krishna and Muniyal (2015) state that mobile computing offers a computing environment over physical mobility. The user of a mobile computing environment will be able to access data, information or other logical objects from any device in any network while on the move. To make the mobile computing environment ubiquitous, it is necessary that the communication bearer is spread over both wired and wireless media. Although there are many advantages of mobile computing, it has

some drawbacks. The most serious drawback is security. Mobile computing has introduced new security challenges that were non-existent in traditional computing. Mobile computing diagram is illustrated in figure 2.1.



Figure 2.1: Mobile computing

2.3 SECURITY ISSUES IN MOBILE COMPUTING

There are limited studies that focus on the users' knowledge and understanding of security on mobile computing in South Africa. There is a lack of results with regard to consideration of users' knowledge, understanding and reactions in South African communities to designate the need for research in this field (Ophoff & Robinson, 2014). There is a gap in the literature as to how mobile computing security influence South African communities to use new technology. Existing literature does not show whether South African communities are security cautious on the internet and are applying all the security measures properly regarding their privacy.

According to Srivastava (2013), numerous security vulnerabilities and threats such as malignant codes are known to the various mobile devices. Hence, applications being used in these mobile devices may cause privacy issues for mobile users. Therefore, both users and the

data that they carry have become a mobile component in computing and have introduced a set of security problems to that in traditional computing.

Mobile devices should be given serious consideration on the issue of security, because it acts as an obstacle in the mobile computing field and adoption of technology in South African communities. There are limited studies that focus on the users' knowledge and understanding of security for mobile computing in South Africa. In addition, it remains uncertain whether the existing security tools, mechanisms and methods are in line with the new technologies and security issues.

A study conducted by Singh, Yerma and Bhart (2016) on consumer behaviour and perception regarding m-commerce in Indian Business to Consumer (B2C) retail. They tested a model based on Technology Acceptance Model (TAM) by investigating the effect of recommendation systems, information search, security systems, regulation systems and virtual experience on perceived usefulness and perceived risks as well as their eventual effect on trust and on the consumer's buying intentions in B2C mobile commerce (M-commerce) retail context. They found that perceived risk is a main influence of Trust as compared to perceived usefulness in m-commerce in Indian context.

According to Thirumoorthy (2015), mobile computing is a versatile and potentially strategic technology that improves information quality and accessibility, increases operational efficiency, and enhances management effectiveness. Information flows through wireless channels in mobile computing. The processing unit is free from temporal and spatial constraints. A processing unit (client) is free to move about the space while getting connected to a server. This is a powerful facility that allows users to get to data site independently. The working of mobile computing has its basics in Personal Communication Systems (PCS's). PCS refers to a wide variety of wireless access and personal mobility services. PCS includes high-tier cellular systems and low tier cellular systems.

Mobile computing affects the entire spectrum of issues in computing. It leads to problems such as searching for current location of a mobile node and imposes a communication structure among nodes to arise (Dudhe & Ramteke, 2014). Mishra and Sah (2016), affirm that security is a prerequisite for every network. However, mobile computing presents more security issues than traditional networks due to the additional constraints imposed by characteristics of wireless transmission and the demand for mobility and portability. Abid (2016) affirm that

mobile computing faces various security issues such as connectivity, information sharing, authentication and data access. Information sharing issue in mobile computing greatly damages users' mobile as well as personal security in mobile computing as usually users save their passwords and logins to exclude the process of re-entering the information repeatedly to save their time.

The fact that both users and the data they carry have become a mobile component in computing has in itself introduced a set of security problems different to that in traditional computing in which precautions have to be taken (Singhal, Singh & Mathpal, 2015). The mobility of users and the data they carry introduces security problems from the point of view of the existence and location of a user (Rani & Rani, 2014). According to Rani and Rani (2014), mobile computing comes with threats to the user and to the corporate environment from personal information to corporate data, mobile devices are used for a wide range of tasks by individuals and companies. Mobile security has become increasingly important in mobile computing. It is a particular concern as it relates to the security of personal information now stored on the smart phones as communication tools but also as a means of planning and organizing their work and private life (Dhingra, 2014).

Alotaibi and Albar (2016) conducted a study on mobile computing security issues and requirements; they highlighted some of the security issues related to mobile computing systems in order to avoid or reduce them, with addressing the security issues into transmission of information over wireless networks and the information residing on mobile devices. Therefore, they found that confidentiality, integrity, availability, vulnerability, non-repudiation, authorization and anonymity are mobile computing system security aspects.

Bilic (2017) indicates that within the context of socio-technological revolution, the rise of virtual reality technology raises new security risks not only to digital information, but also to users' physical well-being. While these applications collect and store increasingly sensitive data, mobile malware is constantly evolving and becoming more complex, reinforcing the importance of and need for secure mobile computing.

Prasanna and Krishnaiah (2013) conducted a study on next generation mobile computing, whereby they mentioned that mobile computing today is hampered by many debilitating factors, such as slow networks, wasteful protocols, disconnections, weak terminals, immature

IP access to networks, poorly optimized operating systems (OS) for mobile applications, content conversions from wired to wireless networks.

2.4 USERS AND MOBILE COMPUTING

Security is the degree of resistance to or protection from harm (Bagdasarian, 2015) and it applies to any vulnerable and valuable asset. Security consists of various categories such as physical security, viruses, and vulnerabilities in software and criminal behaviour (Psannis, Xinogalos & Sifaleras, 2014). The security costs are often perceived as too high, which creates the perception of security mechanisms as obstacles that should be avoided. Changchit (2014) defines security as the degree of protection against loss, damage and criminal activity; he also stated that having security awareness is an important issue for all individuals who are dealing with sensitive data in everyday life.

Mahesh, Jayawant and Kale (2015) mention that when mobile users communicate through mobile computing they should ensure the messages are kept secret, that each party knows who the other party is, the messages are passed from sender to receiver unaltered or modified. In addition, it should detect, prevent and reject any unauthorized resending of messages and neither party can later claim that the exchange did not take place (Saleh & Mashhour, 2014). Yao, Verima, Kang and Sezer, (2017) mention that users have become more mobile where data is now distributed across several locations which has evolved the existence of threats. Hence, hackers became smarter and internet access from any device has grown to be most difficult to control as users can connect to various networks at various locations. This have caused the scrutiny of the security to change over time. Moreover, it bridges the fissure between the physical and the digital worlds that enables a deeper understanding of user preferences and behaviours.

Ibukun and Daramola (2015) point out that for understanding users it's necessary to bridge the distinguished disconnect between security managers and users in creating more effective and workable security measures, as well as upholding good security practice by ensuring cooperation and engagement. Whilst increasing users' knowledge can improve compliance with good security practices. North, Johnston & Ophoff (2014) specify that during the mobile communication, information security and privacy must be considered as an important concern for modern enterprise and individual end-users who perceive their information to be private and worth protecting. Consumers are increasingly using mobile devices for sensitive tasks such

as email, banking and purchasing goods and services online. Security awareness influences users' attitude to information security and their behaviours. With the use of smart phones rapidly increasing, these smart phones face several threats same as traditional computers, but are different in that they are prone to physical loss and theft.

Mobile communication is extremely vulnerable to security risks. With the use of mobile phones, many mobile applications transmit data without encryption and unencrypted data is very easily intercepted during data transmission (Chuchuen, 2016). Chen and Dai (2014) show that security concern has been a major obstacle to mobile commercial transactions. Security concern is defined as users' level of worry and fear about breaches of data confidentiality, integrity and authentication when using information technology. Security concern is a type of psychological anxiety and fear pertaining to security distress impacted their protective behaviour on the internet.

2.5 E-APPLICATIONS

2.5.1 WHAT IS E-APPLICATIONS

According to Markhasin (2017) and (Abu-assi, Wu, Moran & O'Neill, 2016), e-applications refer to electronically/ network based applications for the social development of communities/ societies such as e-learning, e-commerce, e-governance, e-health, e-banking, e-payment.

2.5.2 TYPES OF E-APPLICATIONS

Technology development, particularly in the area of Information Technology (IT) revolutionises the way business is done, the way people conduct their daily activities since the internet, plays an important role in our daily lives.

(I) E-banking

E-banking, also known as internet banking, is a service provided by the banks that gives the customers the ability to do their banking errands online using computers or mobile phones via the internet (Ramavhona & Mokwena, 2016). Internet banking is a banking service that gives consumers a platform to perform banking functions online. According to Soh and Hong (2014), internet banking can be considered as an internet portal through which customers can use different kinds of banking services. Soh and Hong (2014) show that the growth in the use of

internet banking will also change the structure and amount of investment in growth of the banking system.

Today, internet banking is the most innovative and effective way to perform banking transactions instead of using traditional banking (Ahmed & Phin, 2016). The movement and switch from the formal traditional banking environment to internet banking has increased. Despite the benefits of online banking/ e-banking, e-banking has also raised many security issues (Alsayed & Bilgrami, 2017). These security issues often discourage customers from using online banking due to the fear of putting their financial assets at risk (Leukfeldt, Kleemans & Stol, (2016), Razak, 2016).

(a) Challenges of e-banking

A study conducted by Khatri and Upadhyay-Dhungel (2013) highlight that the awareness about internet banking and its benefits and security was identified as the major reason behind less utilization of e-banking among customers. Customers' education levels, their knowledge about the computer and internet, electricity problems and theft of password, and internet infrastructure in the country were identified as major challenges faced by the bank regarding the development of their online facilities.

Identifying factors that affect individuals' intention to adopt e-banking, enables financial institutions to respond properly towards these factors and use their marketing strategies to promote an e-banking system that meets the needs of customers (Singh, Yerma & Bharti , 2016). These factors include reliability, aesthetics, security and credibility, access, ease of use, competence and so forth.

A study conducted in Saudi Arabia by Bushra (2016) shows that banks have started offering online banking services to their customers, but some of them did not feel safe to deal with their confidential information online. However, the main reasons for the customers' concerns are lack of security and usability awareness. In addition, security and usability are important factors that can affect the adoption of e-banking services anywhere, anytime. Also, Bushra (2016) highlights that there is a need for a set of standards to ensure that the best securing practices are adopted and an adequate level of security is attained.

Security is a significant issue in commercial bank management and is connected to a large number of bank activities (Bilan, 2013). E-banking security is a complex system that includes

many activities such as single sign on and multi-factor authentication systems (mobile/web apps, OS logins), standard applications (payment verification services, user authentication services, pc/tab/ mobile login with single sign on, app specific login) (Belas, Koraus, Kombo & Koraus, 2016). For financial institutions to achieve their goal of getting customers to adopt e-banking, they should add customers' evaluations of ease, safety and privacy of m-banking services (Goswami, 2017).

Prior studies have been done on e-banking in Malaysia (Soh & Hong, 2014), in India (Shankar & Kumari, 2016), in Greece (Santouridis & Kyritsi, 2014) and among the South African internet banking studies were carried by Maduku (2014), Ramavhona (2014), Wentzel, Diatha and Yadavalli (2013) as well as Ramavhona and Mokwena (2016). Unfortunately, these prior studies on internet banking adoption in various countries have produced mixed results that have added to the difficulty in articulating the drivers of internet banking adoption (Me, 2017).

(b) Benefits of e-banking

Since the banking sector is a service-oriented business, the appliance of contemporary technologies is necessary to improve the quality of services (Karim & Chowdhury, 2014). Actually, the development and application of the state-of-the-art information and communication technologies (ICTs) have enabled the banking institutions to create sophisticated products and to raise the quality of their services on a much higher level.

Boshkoska and Sotiroski (2018) points out that the application of such new technologies results in many benefits for banking institutions, including the following ones: reduction of costs, increasing the market share, better communication with the clients as well as development of new products and services. Additionally, according to Drigă and Isac (2014), e-banking includes the following types of services: home banking, PC banking, mobile banking and Internet banking.

Kovačević & Đurović (2014) mention that the advantage of e-banking is that there is no need for installing and using dedicated banking software, all that the customer needs is an Internet access. Hence, the client can perform the banking transactions from anywhere and anytime, as opposed with online banking, where customers can access their bank accounts only by using their personal computers with preinstalled software. It is also worthy to mention that with Internet banking, the transactions data are not kept on the users' personal computers, but

instead on servers in the banks, which implies a significantly higher levels of protection and safety visa-versa the potential misuse of customers data.

Furthermore, E-banking has improved efficiency, convenience and offers checking with no monthly fee, free bill payment and rebates on Automated Teller Machine (ATM), surcharges Credit cards with low rates, Easy online applications for all accounts, including personal loans and mortgages 24 hour account access, Quality customer service with personal attention and also Advantages previously held by large financial institutions have shrunk considerably (Lekshmi, 2018).

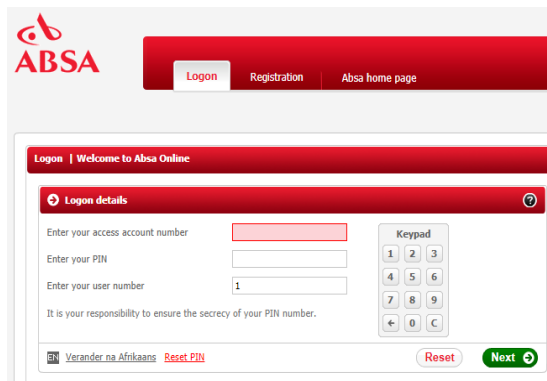
(c) Security mechanisms used for user authentication provided by the leading banking institutions in South Africa

This researcher conducted a review of the authentication approaches offered by banking service providers in South Africa and assessed the practices of the five (5) big banks in South Africa namely: Amalgamated Banks of South Africa (ABSA), Standard Bank Investments Corporation Limited, First National Bank (FNB), Nedcor Limited, Nedbank and Capitec Bank as ranked by BusinessTech (2017). The purpose was to gain tangible results from a field review that investigates and compares different authentication experiences within the e-banking environment. The comparison data was collected by visiting each online banking service of these banks to explore the provided authentication mechanisms. The services were compared on the basis of the following factors:

- **Information based security mechanisms:** these are related to something the user knows such as Personal Identification Number (PIN), username, password or the answer to a secret question (Vaithya, Christy & Saravanan, 2015).
- **Behavioural based biometric mechanisms:** these are related to the pattern of behaviour of a person including signature, key stroke, voice, smell, sweat pores analysis, and measure behavioural characteristics (Kumari, Kaur, Handa & Kaur, 2016).
- **Physiological based biometric mechanisms:** these are related to the shape of the body including facial analysis, fingerprint, hand geometry, retinal analysis, DNA, odour and measure of the physiological characteristics of a person (Kumari, Kaur, Handa & Kaur., 2016).

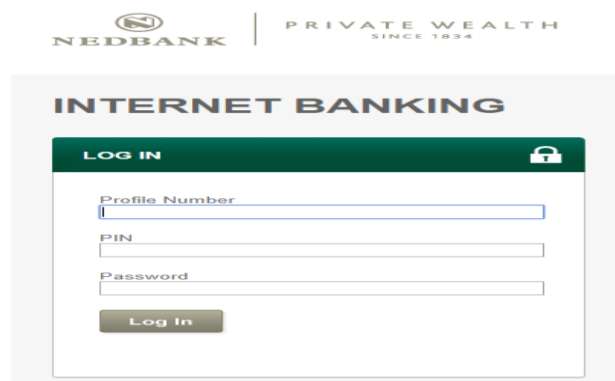
- **Multi-factor security mechanisms:** these are related to something that only each individual user possesses (fingerprint, a voice print, a key fob, a security code) and combines that with another factor, something the user knows (such as the usual username/password login dialog) to prove that he or she is legitimately who they seem to be (Griffin, 2015).

(d) South African top five (5) online banking authentication mechanisms interfaces



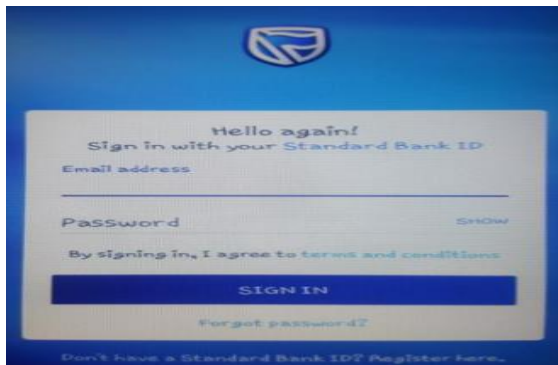
The ABSA Bank login screen features a red header with the ABSA logo and navigation links for 'Logon', 'Registration', and 'Absa home page'. Below the header, a 'Logon details' section prompts users to enter their access account number, PIN, and user number. A numeric keypad is provided for PIN entry. A 'Reset' button is located at the bottom right of the login form. The footer includes the text 'Verander na Afrikaans' and a 'Reset PIN' link.

Figure 2.2: ABSA Bank Login Screen



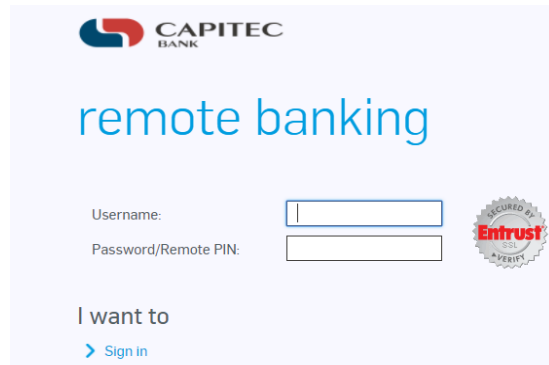
The Nedbank login screen has a green header with the Nedbank logo and 'PRIVATE WEALTH SINCE 1834'. The main heading is 'INTERNET BANKING'. Below this, a 'LOG IN' section contains input fields for 'Profile Number', 'PIN', and 'Password'. A 'Log In' button is positioned at the bottom of the login form.

Figure 2.3: Nedbank Login Screen



The Standard Bank login screen displays the Standard Bank logo at the top. The main heading is 'Hello again! Sign in with your Standard Bank ID'. Below this, there are input fields for 'Email address' and 'Password'. A 'SIGN IN' button is prominently displayed. A 'Forgot password?' link is located below the sign-in button. The footer includes the text 'Don't have a Standard Bank ID? Register here.'.

Figure 2.4: Standard Bank Login Screen



The Capitec Bank login screen features the Capitec Bank logo at the top. The main heading is 'remote banking'. Below this, there are input fields for 'Username' and 'Password/Remote PIN'. A 'Sign in' button is located at the bottom. A 'Secured by Entrust' logo is visible on the right side of the screen.

Figure 2.5: Capitec Bank Login Screen

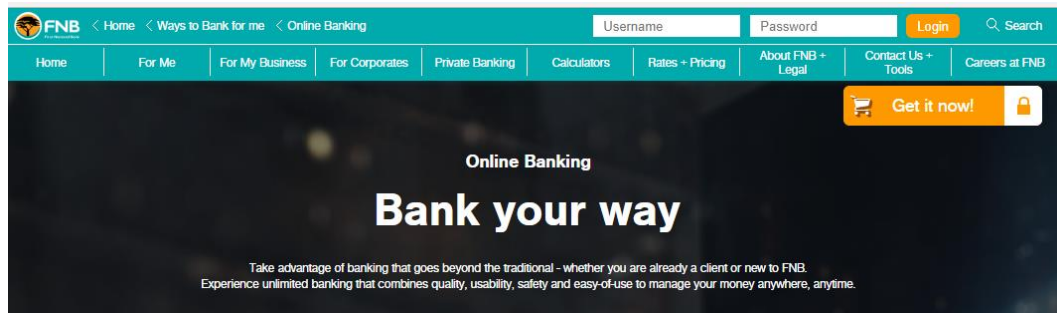


Figure 2.6: FNB Bank Login Screen

Banks use diverse security mechanisms and combinations of them. Nevertheless, identification mechanisms are not standardized. Choubey and Choubey (2013) evaluate the authentication procedures and other security features used by major banks in seven English-speaking countries. Their study revealed that banks use very different approaches to security, from simple usernames and passwords to fairly complex structures with one-time password generated by an external device. This diversity can be problematic for users when they want to change banks or when they are doing business with several banks.

Despite the fact that several methods of authentication, such as hardware tokens, biometrics, mouse and keyboard keystroke analysis, have been developed in the past few years, a simple password-based is still the primary means of authentication for many online services (Koo, Wattt & Chung, 2014). Shende, Sarode and Ghonge (2014) affirm that biometric mechanisms are more secure, because each person has a unique characteristics identification. Additionally, biometric mechanisms are more secure than other security mechanisms like password, PIN or card and key. It also measures the human characteristics and as such it doesn't require users to remember password or PINs that can be forgotten or to carry cards or keys that can be stolen.

Alsaiani, Papadaki, Dowland and Furnell (2014) state that the design of a secure and efficient user's authentication scheme is one of the major concerns. In addition, they suggest that there should be standardization of security mechanisms by the banks. Regarding security, standardization would facilitate the development of interfaces that would prevent phishing attacks. It would also be easier to upgrade the standards and to achieve better protection against different mechanisms of interruptions.

Based on the analysis of identification of the mechanisms of the online and mobile banking, Choubey and Choubey (2013) suggest a combination of these mechanisms in order to facilitate the use of banking services and to find the optimal mechanisms and ways for its

standardization. Authors Svilar and Zupančič (2016) in their study found that respondents regard security as a major principle of satisfaction; also the majority of users consider additional passwords to be necessary. Regarding the security of online and mobile banking, respondents are more cautious. Lastly, the average users do not have enough understanding of how the security features work and are not aware of what they can do to contribute to the greater security of internet and mobile services that they are offered.

(e) South African users' perceptions on e-banking

A study conducted by Maduku (2014) indicates that although customers have a positive attitude towards both internet banking and cell phone banking, their overall attitude towards cell phone banking is more positive than that of internet banking and they are not only more emphatic in their intention to start/ continue using cell phone banking but also to increase their frequency of usage. A previous study carried out by Ramavhona and Mokwena (2016) shows that South African users disagree with the notion that internet banking is as safe as traditional banking (visiting the bank branches). Correspondingly, the majority have intentions to use internet banking services in the near future. It has been found that the majority of respondents from rural areas have never used internet banking due to customers' lack of resources such as mobile devices with internet access and cost (Ramavhona & Mokwena,2016).

Furthermore, security and the complexity of internet banking were revealed as some of the factors hampering the intention to adopt internet banking in South African rural areas. Customers in the rural areas perceived internet banking as unsafe, not having enough security measures to protect customers and that internet banking is difficult to use and not user-friendly (Ramavhona & Mokwena, 2016). Meanwhile, a study conducted by Singh and Masuku (2014) highlight that South African users will not perceive internet banking services as useful and easy to use if their trust in the banks that offer the services is low. Moreover, building customers' trust in the financial institutions offering internet banking services must be a fundamental element of any strategy aimed at increasing their perceptions of usefulness and ease of use.

In addition, South African banks and other banks operating in similar economic contexts should take their relationship with marketing efforts seriously if they are to succeed in building their customers' trust in their institutions. Singh and Masuku (2014) state that increased trust will correspond to an increase in customers' perceptions of the usefulness of internet banking as well as ease of using the system.

(ii) E-learning

E-learning is defined as a training initiative that facilitates materials for learning and communication and delivers course contents electronically with the help of technology mediation (Baskaran, Mahadi, Rasid & Rizal, 2017). Alsaiari, Papadaki, Dowland and Furnell (2014) refer to e-learning as the use of electronic technology in education via computer and the internet. Unlike many challenges such as time and space limitations faced in traditional training methods, the training and accessible of materials can occur anywhere and at any time. E-learning is considered to be one of the most important tools in the field of education, involving distance training through electronic media, as noted by Baskaran, Mahadi, Rasid and Rizal (2017). Serb, Defta, Iacob and Apetrei (2013) state that e-learning is a learning environment supported by continuously evolving, collaborative processes focused on increasing individual and organizational performance.

Adetoba, Awodele and Kuyoro (2016) mention that organizations such as universities and colleges have shown a remarkable tendency to offer e-learning courses. The potential of e-learning is to provide services in the form of same time learning “live” and not same time learning classes, also blended learning to a large number of learners who are directed towards life-long learning. E-learning users focus on how to benefit from e-learning for their teaching and learning purposes (Arkorful & Abaidoo, 2014).

According to Nyeko and Ogenmungu (2017), there are some concerns for the slow adoption of an act in e-learning witnessed in higher institutions of learning in developing countries due to some noteworthy barriers hampering their efforts compared to developed countries.

(a) Challenges of e-learning

Many institutions are rushing into adopting e-learning platforms without carefully planning and understanding the ever-present security concerns. Issues such as legitimate users, course content reliability and accessibility including the availability as well as other considerations all need to be carefully addressed in order to ensure that the learning process can effectively take place (Serb, Defta, Iacob & Apetrei, 2013). The demand for e-learning systems in both academic and non-academic organizations has increased the need to improve security against impersonation fraud.

In e-learning systems, it is evident that due to the variation in authentication strength among controls, a 'one size fits all' solution is not suitable for securing diverse e-learning activities against impersonation fraud (Beaudin, Levy, Parrish & Danet, 2016). With increasing demands being placed on the learning education sector, enhanced means of protecting personal identifying information through added security measures is needed. According to Marnell and Levy (2014), gaining secure access to course content areas through possession of held objects, knowledge or physical characteristics has accelerated significantly through a multitude of consumer devices, services and e-learning interfaces. However, this expansion of methods to gain authentication has resulted in a battle of supremacy between usability, memorability of passwords, securing of personal information, e.g. Identity Document (ID).

According to Osman (2017), technical challenge is considered to be the most important challenge facing the adoption of e-learning. To avoid these challenges, strong updated infrastructure should be available including modern technology, fast internet connection, continuous power supply, security, regular maintenance and efficient administration. According to Asmaa and Najib (2016), the sharing of information, collaboration and interconnectivity are core elements of any e-learning system. Data must then be protected in order to maintain confidentiality, integrity and availability. Protecting against data manipulation, fraudulent user authentication and compromises in confidentiality are important security issues in e-learning.

Asmaa and Najib (2016) indicate that every student must be aware of each and every document received from institutions, teachers or other students. Storing login information (username and passwords), provides a big opportunity for an attacker to prevent an authorized learner from accessing the e-learning server. Among all authentication mechanisms like passwords, smart cards, digital signatures and digital certificates, there is no guarantee that dishonest students will keep their password secret (Savulescu, Polkowski, Cosmin & Elena, 2015). Passwords might be misused at the time of submission of an assignment, receiving question papers, downloading course material and so forth, where biometric authenticity would give better security. Biometric mobile device authentication has an advantage since it is based on something that is not easily copied or stolen (Sayed, Traore, Woungang & Obaidat, 2013).

(b) Benefits of e-learning

E-learning has developed and now we embrace mobile devices such as smartphones, tablets and iPads in the classroom and office as well as using a wealth of interactive designs that make

distance learning not only engaging for the users, but valuable as a lesson delivery medium (Chen & He, 2013). E-learning offers everyone the opportunity to become a learner. The concept of anytime, anywhere learning promotes life-long learning and accordingly eliminates the problems associated with distance (Riahi, 2015). The flexibility that e-learning offers students is the main motivating factor in choosing online courses. Furthermore, the usage of technology in learning will provide other advantages, such as improving the quality of learning, improving access to education and training (Lin, Lu & Liu, 2013).

E-learning provides a platform of a well-designed, learner-centred, engaging, interactive, affordable, efficient, easily accessible, flexible and meaningfully distributed and facilitated e-learning environment (Bandara, Loras & Maher, 2014). In addition, students can save money and time spent on travelling and getting the right materials for their study. They can reduce printing costs by reading the available learning materials online (Dai, Andras & Zoltan, 2016). Also e-learning increases access to e-learning materials and enables students to have wider access to limited resources, such as e-journals and e-books. Another benefit offered by e-learning is faster delivery of assessments as lecturers can give feedback faster compared with the traditional method, and students can also contribute to feedback amongst themselves (Hashemi & Hashemi, 2013).

(c) South African users' perceptions on e-learning

A study conducted by Bagarukayo and Kalema (2015) noted that the e-learning potential to unfold as a true socio-technical network was not fully realised and the technical aspect was not engaged at a socio-technical agency. According to Isabirye and Dlodlo (2014) in their study they found that self-regulating e-learning as an intervention for poor results in science subjects leads to improved learners' grades. It provides multimedia and simulation materials, is self-paced, self-regulated, learner-led and encourages knowledge constructions that leads to better performance in science subjects. The e-learning intervention shows positive results, especially for high potential learners, among challenges of equipment issues and lack of prior basic IT skills. Issues of incomplete marks made a full detailed analysis of grade performance difficult and provided no correlation between assessment scores with relevant statistical information.

A previous study conducted by Sibanda and Donnelly (2014) determined the impact of e-learning on performance, showing that learners' performances increased after the introduction of online learning as years progressed and learners became academically more engaged as they

became more familiar with the online learning platform. Younger learners quickly adapted and became engaged which improved performance. Cijina and Saartjie's (2016) study specify that the expectations of the development team did not cascade down to the users' level so that the user experience was different from the designed experience. This is indicative of one of the major gaps that will be prevalent if a readiness assessment is not performed prior to the rollout of e-learning. Due to the absence of a readiness assessment having been done, various retrospective design and process changes to the e-learning system are required in order to meet expected learning outcomes.

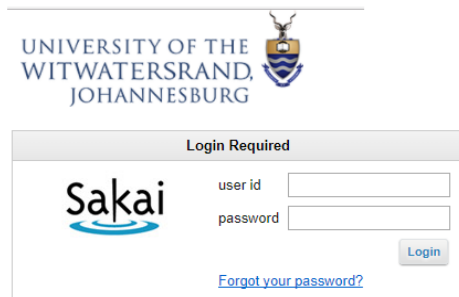
A study conducted by Tshabalala, Ndeya-Ndereya and Van Der Merwe (2014) highlight that the Faculty of Education staff were not utilizing the facility that could have been instrumental in the use of blended learning. Furthermore, findings indicated that this was a result of a failure to plan properly for the implementation, monitoring and evaluation of blended learning. Additionally, it seems that the learning management system (Moodle) is not assisting students who are supposed to be primary beneficiaries, probably due to uncoordinated efforts to implement blended learning in the Faculty of Education.

(d) E-learning systems used by five (5) South African universities ranked among the world's best universities

University of the Witwatersrand uses Wits-e that is an open source, interoperable enterprise ready platform for e-learning and collaboration at Wits (Wits, 2017). The University of Cape Town uses Vula that is an official online learning system that houses websites for academic courses, student societies, study and research groups, faculty and departmental groups as well as assorted projects and initiatives (UCT, 2017). Stellenbosch University uses Sun Learn that is an open source, powerful flexible and mobile-ready blended learning platform for learning and teaching; the system is easy to learn and use for both staff and students (Stellenbosch-University, 2017).

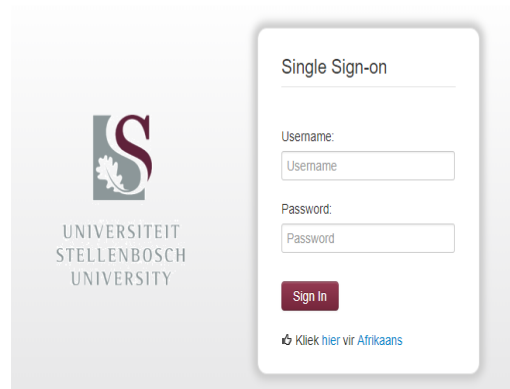
University of Kwazulu Natal uses Moodle/Learn that is an online learning management system utilized by staff and students to maximise the teaching and learning potential (UKZN, 2017). University of Johannesburg uses Blackboard that is a management system at University of Johannesburg (UJ) for accessing academic modules, communities and announcements. To gain access students and staff login through the ULink portal. Tools available in Blackboard modules include content areas, capable of hosting class presentations, documents, web links,

assignments, plagiarism tools, online tests, wikis and reflection diaries and so forth (UJ, 2017). Below are the various e-learning authentication interfaces for the above mentioned e-learning systems.



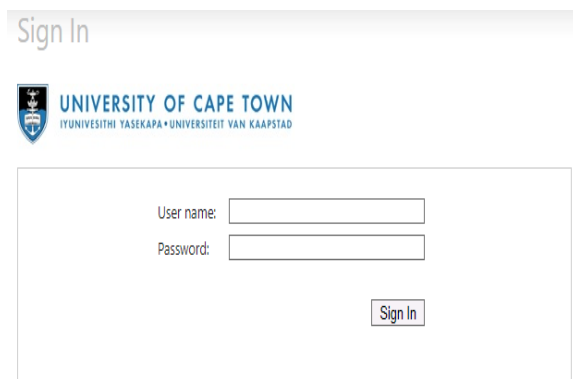
The interface for the University of the Witwatersrand (Wits) Sakai system. It features the university's logo at the top. Below it, a 'Login Required' box contains the Sakai logo, a 'user id' input field, a 'password' input field, and a 'Login' button. A link for 'Forgot your password?' is located at the bottom of the login box.

Figure 2.7: Wits-e Security Interface



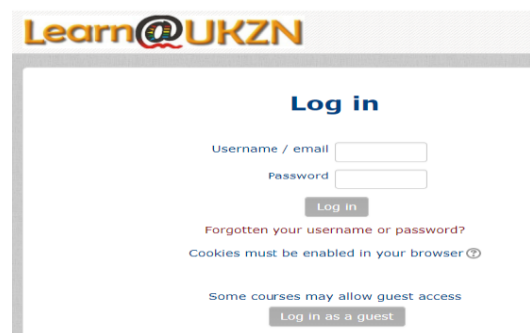
The interface for Stellenbosch University's Sun-Learn system. It displays the university's logo on the left. On the right, a 'Single Sign-on' box contains a 'Username' input field, a 'Password' input field, and a 'Sign In' button. A link for 'Kliek hier vir Afrikaans' is at the bottom of the sign-on box.

Figure 2.8: Sun-Learn Security Interface



The interface for the University of Cape Town's Vula system. It shows the university's logo and name at the top. Below, a 'Sign In' box contains a 'User name' input field, a 'Password' input field, and a 'Sign In' button.

Figure 2.9: Vula Security Interface



The interface for UKZN's Moodle/Learn system. It features the 'Learn@UKZN' logo at the top. Below, a 'Log in' box contains a 'Username / email' input field, a 'Password' input field, and a 'Log in' button. Links for 'Forgotten your username or password?' and 'Cookies must be enabled in your browser' are present. At the bottom, there is a 'Log in as a guest' button.

Figure 2.10: Moodle/Learn Security Interface



The interface for the University of Johannesburg's ULink system. It shows the university's logo at the top. Below, a 'uLink Sign In' box contains a 'University Login ID' input field and a 'Password' input field. A list of links is provided: 'Sign in', 'Reset password', 'Create password (Students)', 'uHelp', 'About uLink', and 'How to connect to WiFi'. At the bottom, it says 'Your gateway to institutional resources!'.

Figure 2.11: ULink Security Interface

(iii) E-commerce

According to Kurnia, Choudrie, Mahbubur and Alzougool (2015), e-commerce is defined as the integration of a company's business, including products, procedures and services over the internet. It enables the buying and selling of products and services through the shorefronts. It is about using the convenience, availability and worldwide reach to improve existing businesses or to create new virtual business. Furthermore Hussein and Baharudin (2017) refer to e-commerce as the process of buying, selling, transferring or exchanging products, services and information through computer networks, principally the internet. E-commerce is fundamentally an (additional) sales channel, the key features of which are speed, flexibility and transparency.

According to Sabri et al. (2015), e-commerce provides greater opportunities to businesses such as greater visibility, broader market reach, reduced warehousing costs, shorter delivery times, more efficient procurement processes and higher customer satisfaction. The fast growth of internet adoption and usage everyday has increased the demand on online services in every sector; this new movement has restructured the marketplace and the business relationships among businesses and individuals (Sabri, Sulaiman, Ahmad & Tang, 2015). Hussein and Baharudin (2017) affirm that adopting the online services by businesses and individuals has become almost mandatory in the current fast growing digital.

Lekhanya (2016) mentions that use of e-commerce by rural communities is somewhat complicated. It is found that the availability and use of appropriate e-commerce technologies extend beyond provision of access to provision of support outside technology and multi-stakeholder approach to addressing the economic situation of rural communities. According to Madhushi and Fernando (2016) as a business, when they step into Ecommerce, they need to protect their online transaction securely with privacy safety and trusting issues that come up with different types of intruders. Implementing E-commerce gives these kinds of benefits. This may be impossible without a coherent, consistent approach to E-commerce security. E-commerce always does its transaction between customers using the internet for the reason that the business should have a high-end security system and should have a good privacy control system.

(a) Challenges of e-commerce

According to Madhushi and Fernando (2016), E-commerce offers many benefits as well as problems that Small and Medium-sized Enterprises (SMEs) need to be aware of and deal with in an efficient way. There are many issues as well as the perceived needs concerning SMEs that require changing their business strategy to e-business technology. Moreover, the risk to transform from traditional business strategy to new strategy is rather high.

Mostly failure to secure transactions, infrastructure or network externalities may cause people's resistance in adopting and using e-business applications. Additionally, the slow progress of e-business technology adoption may be associated with the level of intellectual and social capital within the SMEs, such as issues relating to senior management championship, company history, organizational culture and age profile (Sharabati, Shamari, Nour, Durra & Moghrabi, 2016).

According to Madhushi and Fernando (2016), e-commerce security has its own specific subtleties and is one of the most noteworthy obvious security parts that influence the end client through their everyday instalment association with business. E-business security is the insurance of e-trade resources from unapproved access, use, modification, or annihilation. According to Singh (2014) in e-commerce security challenges, poor security on e-commerce web servers and in clients' personal mobile devices is centre issue to be determined for fast development of e-commerce. Gautam and Yadav (2014) state that data security is a fundamental administration and specialized necessity for any proficient and successful payment exchange exercise over the e-commerce. Educating the customers on security issues is still in the earliest stages of organization, yet will turn out to be the most basic component of the e-business security design.

(b) Benefit of e-commerce

According to Ombati and Omulo (2017), adoption of e-commerce offers a great opportunity for small and medium enterprises to gain many benefits such as improved productivity by creating new relationships through customers or suppliers and other strategic partners. Authors Ombati and Omulo (2017) went on by stating that adoption of e-commerce also improved cost saving in transaction costs and increased the speed of business as well as improved transaction efficiencies and access to a wide range of markets.

Banoobhai-Anwar and Keating (2016) predict that the internet will continue being relevant even in the new knowledge economy because it removes communication barriers that prevent seamless interactions among companies, for instance language, culture and geographical distance. With e-commerce, organizations can easily communicate, share information and do business rapidly and conveniently.

E-commerce provides customers with a variety of choices for products or services. It enables customers to access products and services on a 24/7 basis uncontained by geographical boundaries and moreover, customers receive updated information and are allowed to exchange ideas and experiences (Banoobhai-Anwar & Keating, 2016). E-commerce expands geographical reach for organizations so that organizations can have customers across the country and around the world. It reduces marketing and advertising cost; internet marketing targets specific customers and organization brand image gets improved (Banoobhai-Anwar & Keating, 2016).

(c) Users' perceptions on e-commerce by South African residents

In a study conducted by Lekhanya (2016), in South Africa (Kwazulu Natal) the research found that the majority of respondents do not use e-commerce to purchase Small and Medium-sized Enterprises (SMEs) products with about half of respondents indicating that they still do not agree that ecommerce can change their buying behaviour. However, on the other hand, many respondents believe that e-commerce is more cost effective, safe and important for the improvement of rural consumers, but this does not mean that they are using it.

Furthermore, the results indicate that most of the respondents believe SMEs' owners/managers lack corporate government orientation due to lack of qualified members of the corporate sector in their business leadership structures. Therefore, partnership with government agencies is encouraged as this will help them in limiting the skills gap and shortage of human capital in rural Small and Medium-sized Enterprises (SMEs) sector in South Africa. This study found that many people don't believe ecommerce is more convenient indicating the need for Small and Medium-sized Enterprises (SMEs) in operating in rural areas to put more effort into direct marketing and consumers education with regard to the advantages of using e-commerce.

Findings of the study conducted by Butler and Butler (2015) revealed that relative advantage and compatibility are the only Diffusion of Innovation variables that significantly influence the

decision to adopt e-commerce in Durban. Specifically improving information exchange with customers, easier access to international markets, expansion of business reach, reduction of costs of maintaining up to date company information and improving information exchange with suppliers are significant factors that inform the decision to adopt e-commerce in Durban.

In addition, Butler and Butler (2015) state that compatibility with existing company's technology infrastructure and compatibility with company values significantly affect SMMEs' decision to place orders with suppliers through the internet. Interestingly, the adoption of the other e-commerce options (online payment by credit card, online ordering and online customer services) is not significantly influenced by compatibility. The findings imply that in order to increase Small, Medium and Micro-sized Enterprises (SMME) e-commerce adoption, SMMEs need to be better acquainted with the benefits that derive from its adoption. Moreover, a stepwise approach to e-commerce adoption is advised, starting with e-commerce options that are compatible with SMMEs technology infrastructure and values, then gradually moving to more sophisticated e-commerce options.

(d) The best rated e-commerce stores in South Africa

The best e-commerce stores in South Africa ranked by BusinessTech (2017) include Yuppiechef.com ranked as the best e-commerce store and best shopping process. Takealot.com ranked as South Africa's favourite e-commerce website, followed by Action Gear ranked as best customer service. In addition, Bidorbuy ranked as best e-commerce service platform. Lastly, Kapas Baby and Toddler ranked as best small e-commerce. Both e-commerce stores use common security authentication which is knowledge based security mechanisms. According to Vaithyasubramanian, Christy and Saravanan (2015) knowledge based security mechanisms are related to something the user knows, such as Personal Identification Number (PIN), username, password or the answer to a secret.

Lal, Prasad and Farik (2016) affirm that the **something you know** mechanism is the most common mechanism used and can be a password or a simple personal identification number (PIN). However, it is also the easiest to beat. When using passwords, it's important to use strong passwords. A strong password has a mixture of upper case, lower case, numbers, and special characters.

According to Nayak and Bansode (2016), the problem of knowledge-based authentication system is typically text-based passwords that are well known. Users often create the memorable

passwords that are easy for attackers to predict but strong system assigned passwords are difficult to remember for the users. Hence, a password authentication system encourages strong passwords while maintaining memorability. However, password based authentication methods continue to remain the principle method of authentication because of their simplicity and straightforwardness (Skračić, Pale & Jeren, 2014). First, the supplicant enters the username and second, the password. The password is the secret combination of words and numbers which the supplicant knows (Lal, Prasad & Farik, 2016). See figure 2.9 below

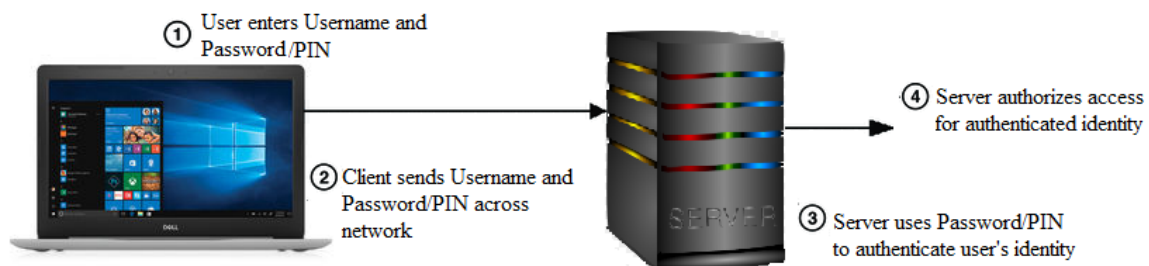


Figure 2.12: The Something You Know Authentication Mechanism

In addition, Passwords are becoming less and less reliable in protecting data and identities. Their management, protection and memorization are becoming increasingly problematic and malicious actors countless ways to steal the, break them, reset them or get past them (Dickson, 2016). Whereas Password authentication does not require the support of hardware as authentication of this type is simple and does not require much processing power (Pandya, Narayan & Thakkar, 2015).

Below are the online security interfaces for the above mentioned e-commerce stores.

KAPAS
for little people

Login

Email Address

Password

[Forgot your password?](#)

Sign In

Figure 2.13: KAPAS Security Interface

YUPPIECHEF Account Login

Email Address:

Password:

☒ Remember me
Stay logged in for 30 days

LOG IN

[Forgot Password?](#) | [New? Create Account.](#)

OR

LOG IN WITH FACEBOOK

Figure 2.44: YuppieChef Security Interface

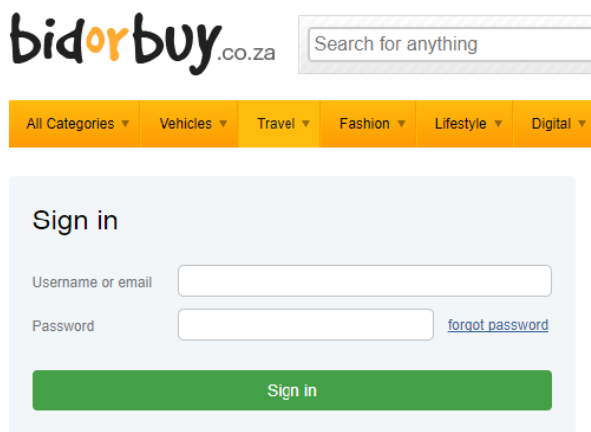


Figure 2.5: Bid or Buy Security Interface

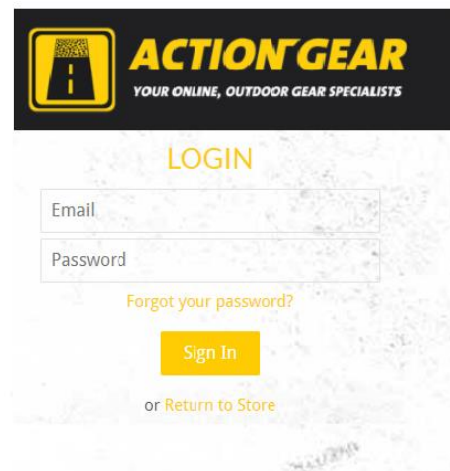


Figure 2.66: Action Gear Security Interface

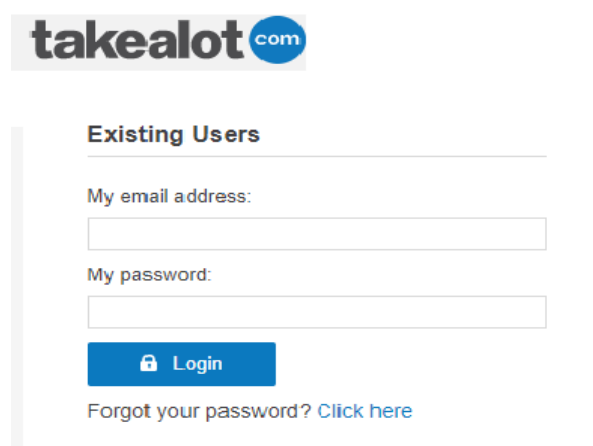


Figure 2.17: Takealot Security Interface

(iv)E-governance

E-governance is defined as the utilization of the internet and World Wide Web (www) for transfer of information and delivery of services from government to citizens Ud din, Xue, Abdullah, Ali, Shah and Ilyas (2017). E-governance helps citizens to reach government services with the help of internet and helps citizens to reach government services with the help of internet. Ud din, Xue, Abdullah, Ali, Shah and Ilyas (2017) mention that e-governance has the potential to reach people through different innovative ways.

According to Jha and Bose (2013), development of e-governance is very necessary and has become a vital need for the community, in this case as a service to its citizens. Therefore, the development and maintenance including networking, security and data confidentiality is very

important to note, whereby various forms of construction, development and security have a lot to offer. It can be used as a rationale to be able to build or develop a form of e-governance reliable systems.

Mohammed et al. (2016) specify that many countries such as Singapore and Australia have adopted e-governance. Furthermore, Mohammed et al. (2016) mention that to ensure better government processes, many governments make provision for having investments in information communication technology; use of e-government online is high in Singapore, Sweden and Norway where people feel comfortable dealing with government this way Mohammed et al. (2016).

According to Salem (2016), An e-governance initiative will remain vulnerable to security breaches in absence of a well-cleared security policy. In addition, Information security policies are the corner stone of information security effectiveness. Data security will help the user to control and secure information from inadvertent or malicious changes and deletions or unauthorised disclosure. Mohammed et al. (2016) consider e-governance as implication of information and communication technology (ICT) in order to improve public services and strengthen support to public policies.

(a) Challenges of e-governance

E-governance is becoming significant and has played a great role in each sphere of the economy over a number of years. However, it still has some hurdles to overcome regarding e-governance such as digital divide between urban and rural, poverty, illiteracy, security and cost of implementation (Oppermann, 2016). Each of these issues and challenges are posing serious concerns to government. Furthermore, government should spend more on this (e-governance) initiative to make it transparent, convenient, safer and citizen friendly in order to enhance people's confidence in good democratic e-government (Oppermann, 2016).

According to Verkijika and De Wet (2016), security and reliability concerns are identified as very important factors influencing consumer risk perceptions of the issue of security effectiveness and perceived security control. Furthermore, consumers believed that e-service provision of accurate and reliable services would contribute to the adoption of e-services. Rao and Iyer (2016) state that web applications, especially dynamic applications, are more complex as compared to traditional applications. In particular it is very challenging to the government as they have neither certified nor trained staff in developing and testing the web applications

security area, even though it is essential. Additionally, the challenge to the government is how to implement technology to strengthen confidence in privacy measures by creating mutual transparency between public administration and citizens.

According to Hassan and Khalifa (2016), privacy and security of information are priority issues in dealing with e-governance; most of e-governance applications depend on internet to deliver a widened service for citizens; the increased transparency and easier access will be considered as an advantage. To protect e-governance systems, current information security procedures of risk management shall be used, strategies of improving security like security policies, security practices and security procedures must be in place as well as utilization of security technology measures such operational technology, one-time passwords, cryptography, firewalls, analysis tools, monitoring tools that help to protect e-governance systems against attack (Priyambodo, Venant, Irawan & Waas, 2017).

(b) Benefits of e-governance

E-governance reduces the processing costs, improves service delivery and increase transparency and communication between a government and its citizens, also brings advantages to the public resources, promoting better planning and targeting policies to address problems of communities and provides a massive potential to locate innovative ways to reach the people's satisfaction (Ojo, 2014). Furthermore, the movement of e-governance is significant for government to interact and communicate with people and business transactions. According to Kaur (2016), e-governance provides a paper free environment and improves the structure for delivery information and services to users by using information and communication technology (ICT).

(c) South African users' perceptions on e-governance

A study conducted by Mawela, Ochara and Twinomurinzi (2017) in South African municipalities, revealed that information and communication technology was not seen as an important department like the service departments. Also, within the support departments it didn't have as much clout as compared to more established support functions such as finance or audit. Secondly, the respondents indicated that their most relevant issues were around areas such as a lack of funding, shortage of skills, poor leadership and the profile of information communication technology in municipalities.

Singh's (2016) study shows that the establishment of an e-skills hub in Kwazulu Natal with a focus on e-governance will assist in both the advocacy pull and the technology and artefact push. Also, the evidence of government taking a practical route towards this type of service delivery is clear. A study carried out by Pretorius and Calitz (2014) indicates that putting government online is one thing, making government websites functional and easy to use is quite another. Users interacting with government websites often experience that not enough has been done to anticipate their needs to make information easily available and locatable.

In addition, citizens' higher perception of the usefulness and ease of use of e-governance websites directly enhanced the level of intention of citizens to continue to use e-governance websites. The user experience with government websites does not compare well with the online experience that citizens have in the private sector.

(d) E-governance applications used in South Africa

Online services offer citizens opportunities to conduct transactions with government online without visiting the offices physically; thus saving time and money. Government departments that offer online services include Department of Home Affairs that uses e-home affairs online application for citizens to check the status of their identity documents (ID), passport or permit application, verify their marital status, whether their ID numbers have been duplicated and whether someone is still alive (eHomeAffairs, 2017).

South African Revenue Services (SARS) is using an e-filing online system, which provides the platform to submit tax returns electronically and do a value-added tax (VAT) vendor search. SARS e-filing is a free, online process for the submission of returns and declarations and other related services (SARS, 2017). The Department of Roads is using e-toll. According to SANRAL (2017), e-toll (in South Africa) consists of the electronic toll collection (ETC) processes employed by South Africa's roads agency (SANRAL) on selected toll roads or toll lanes, subject to the SANRAL Act of 1998.

The Department of Labour is currently using uFiling which is described as a free online service that allows you to securely submit your Unemployment Insurance Fund declarations and pay your monthly contributions (uFiling, 2017). It harnesses the power of the Internet allowing Employers of Domestic, Commercial Employers (SMME) and Tax Agents to complete and submit monthly Unemployment Insurance Fund declarations and to securely pay Unemployment Insurance Fund contributions. With uFiling, you as an employer has 24/7

online access to your employee declaration information through the Internet, whether you are at home, the office or abroad. UFiling conveniently brings all these secure services to you as an employer via the Internet.

A screenshot of the 'Customer Login' form. The form has an orange header with the text 'Customer Login'. Below the header are two input fields: 'Customer ID / Username' and 'PIN'. To the right of the 'PIN' field is a 'Verification Code' field containing the code 'FZZ848'. Below the 'Verification Code' field is an 'Enter Verification Code' field. There are links for 'New to e-toll? Create an e-toll account', 'Forgot PIN?', and 'Switch to Account Login'. A 'Login' button is at the bottom right.

Figure 2.78: E-Toll Security Interface

A screenshot of the SARS eFiling login interface. The header features the 'SARS eFILING' logo on the left and 'REGISTER' and 'LOGIN' buttons on the right. The main content area has the text 'Please provide your login details' and 'This is your generated Login Name (ie. johnd8978)'. Below this are input fields for 'Login Name' and 'Password'. At the bottom, there are icons for 'HELP', 'REGISTER', and 'LOGIN', and a link that says 'For a reminder of your Login Name or to reset your password click here'.

Figure 2.19: E-Filing Security Interface

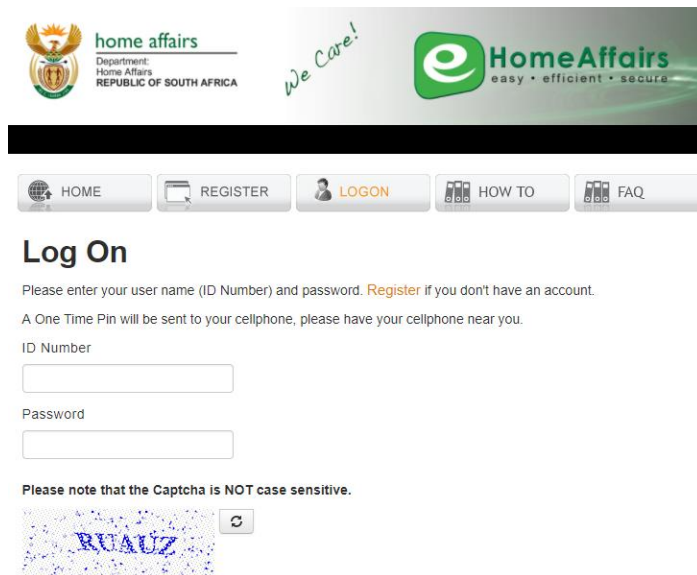


Figure 2.20: E-Home Affairs Security Interface



Figure 2.21: UFiling Security Interface

2.6 TECHNOLOGY ADOPTION MODELS

Mobile computing is a relatively new field of research with little more than three decades of history. During its lifetime, it has expanded from being primarily technical to now also being about usability, usefulness, and user experience. Literature reviews revealed interchangeable use of the terms adoption and diffusion, although these terms are quite distinct from each other. Therefore, noting the difference between these two terms is in order. Adoption refers to the stage in which a technology is selected for use by an individual or an organization (Sharma &

Mishra, 2014), while the term diffusion refers to the stage in which the technology spreads to general use and application (Rogers, 2003).

Therefore, while the term adoption is used at individual level, diffusion can be thought of as adoption by the masses. Since the research on user adoption of information technology was introduced by Fred D. Davis in the 1980s, two critical constructs perceived that usefulness and perceived ease of use in the Technology Acceptance Model (TAM) have generated a long term impact on management and education literature (Hsiao, Chang & Tang, 2016). Many researchers have tried to determine the behavioural factors that influence the individual to adopt and use a certain technology. Theories and models are developed in different disciplines but are then used in predicting, explaining and understanding individuals' acceptance and adoption of new Information system products or technologies (Tarhini, Elyas, Akour & Al-salti, 2016).

Each researcher using a framework to study the adoption has identified elements to measure intention to use and behaviour. Perceived ease of use, perceived usefulness, privacy issues, security issues, enjoyment, and some of the factors mentioned in a previous research conducted by Venkatesh, Morris, Davis and Davis (2003) are going to be discussed in more details in this section. The broad research in the information system field has resulted in a number of theoretical models that have evolved for explaining adoption of technology and are summarized as follows:

2.6.1 THEORY OF REASONED ACTION (TRA)

Theory of Reasoned Action (TRA) was formulated by Fishbein and Ajzen (1975). It is a versatile behavioural theory and models the attitude-behaviour relationships. According to Otieno, Liyala, Odongo and Abeka (2016), the formulation of TRA came forth after trying to estimate the discrepancy that existed between attitude and behaviour. The fundamentals of the TRA come from the field of social psychology. Social psychologists attempt among other things to explain how and why attitude affects behaviour. TRA theory maintains that individuals would use computers if they could see that there would be positive benefits (outcomes) associated with using those (Samaradiwakara & Gunawardena, 2014). TRA aims not only to explain but also to predict behaviour considering beliefs, attitude and intention. Samaradiwakara and Gunawardena (2014) indicate that the TRA is part of social cognition models used to predict human behaviour. Social cognition models use a limited number of cognitive factors, beliefs and attitude as determinants of social behaviour.

Akhavan, Hosseini, Abbasi and Manteghi (2015) state that the power of an individual's intention in behaviour comes from two factors: the attitude toward behaviour and subjective norms that stem from social influence. These factors are mainly affected by an individual's belief, whereby belief about the result of behaviour and the evaluation of the result shapes the attitude. Subjective norms are also under the influence of beliefs. Nadlifatin, Lin, Rachmaniati, Persada and Razif (2016) define attitude as the person's evaluation of the behaviour or action intended while subjective norms are perceived expectations of the person's significant others with respect to the behaviour intended.

The TRA has been used successfully in understanding and predicting human behaviour in a variety of settings. The subjective norm is the second variable weighted for behaviour intention. Myresten and Setterhall (2015) define subjective norm as a person's perception that most people who are important to him or her think he should or should not perform the behaviour in question. Subjective Norm consists of three functions: perceived expectations from other people, the actual motivation to go for these expectations and perform the behaviour, and the number of reference group beliefs (Fishbein & Ajzen, 1975).

Nadlifatin, Lin, Rachmaniati, Persada and Razif (2016) affirm that TRA is formulated in an effort to describe the likelihood that a person's behaviour will lead to a specific outcome; the intention outcome is predicted by attitude and subjective norm. Intention is a representation factor that is able to capture human efforts to perform a particular behaviour. The intention itself leads to a specific action. According to Jani, Sari, Pribadi, Nadlifatin and Persada (2015), Subjective Norm is the perceived social pressure to perform a particular behaviour. Some related model studies mentioned Subjective Norm as the individual perception that is influenced by social environment, which has a significant influence on the individual's performing a particular behaviour (Nadlifatin, Lin, Rachmaniati, Persada & Razif, 2016). The theory can be depicted as shown in figure 2.22.

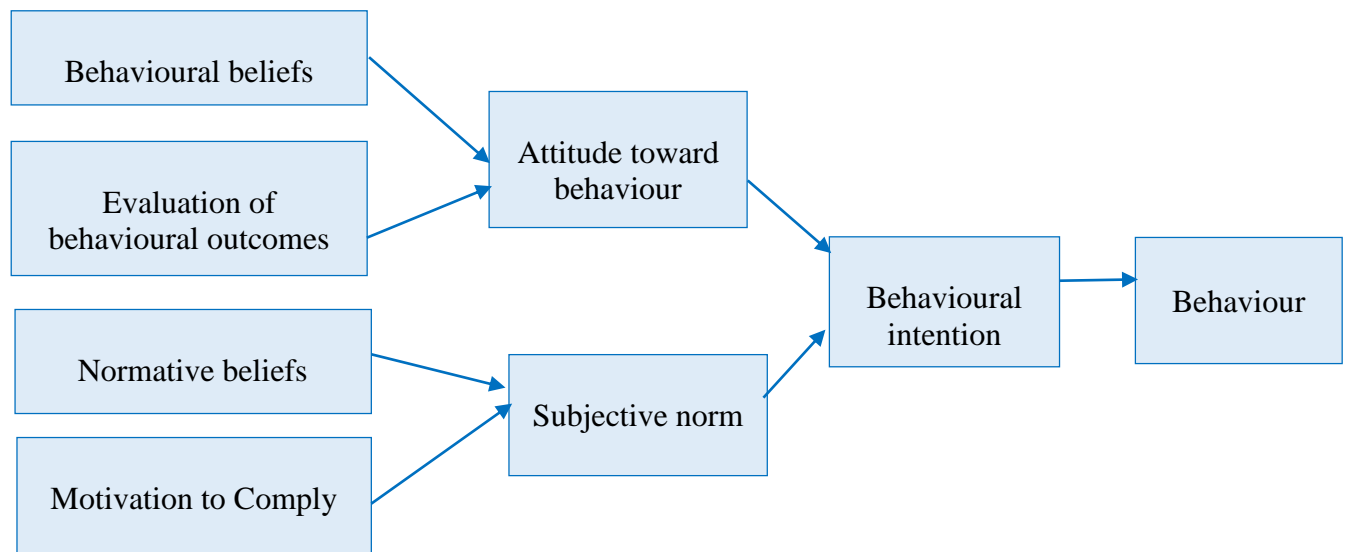


Figure 2.22: Theory of Reasoned Action, source (Fishbein & Ajzen, 1975)

2.6.2 DIFFUSION OF INNOVATION THEORY (DOI)

The Diffusion of Innovation (DOI) is all about getting new ideas adopted; even when it has obvious advantages, it is often very difficult. Diffusion of Innovation theory, consistent with the theory of reasoned action (Buc & Divjak, 2016) define five factors that impact the rate of adoption of innovations: relative advantage, compatibility, trialability, observability and complexity. The factors are positively correlated with rate of adoption, except complexity, which is generally negatively correlated with rate of adoption (Buc & Divjak, 2015). Moore and Benbasat (1991) developed this DOI in Information Technology (IT) and generated eight factors with the effect on IT adoption: relative advantage, compatibility, trialability, image, and voluntariness, ease of use, visibility and result demonstrability.

A comparison of the DOI theories of Rogers (2003); Moore and Benbasat (1991) indicates that the first three characteristics of both are similar in meaning. A relative advantage is the degree to which an innovation is better than current technology. Compatibility is the degree of an innovation matching the existing values, needs and experience of potential adopter. Trialability is the degree to which an innovation can be experimented with before using it. Roger's observability, as the degree to which the outcomes of an innovation are visible for others, is substituted by Moore and Benbasat's (1991) Visibility and Result Demonstrability. Visibility means that the degree of the idea of the innovation itself can be visible. Result Demonstrability

is the “tangibility of using the innovation, including their Observability and Communicability (Juksel, 2015).

Roger’s (2003) Complexity, understood as the relative difficulty to understand and use an innovation, and is replaced by Moore and Benbasat’s (1991) characteristic ease of use. This refers to the degree to which one perceives that adoption of an innovation would be without physical and mental effort. There are two new factors that Moore and Benbasat introduced: Image and Voluntariness. Image is “the degree to which the use of an innovation is perceived to enhance one’s image or status in one’s social system” (Mathur & Verma, 2014). Voluntariness concerns the degree to which the innovation adoption is voluntary or is of free will. Rogers (2003) suggests using Moore and Benbasat's (1991) instruments and various settings for future research in the diffusion of technology innovations.

According to Rogers (2003), diffusion is the process by which an innovation is communicated through certain channels over time among the members of a social system. Azeta and Ibukun (2016) define diffusion as a particular type of connection concerned with the spread of messages that are considered as new ideas. Rogers (2003) explains in his study how an idea or product disseminates among a specific population or social system. Among its achievements, people are part of a social system; they choose a new idea, behaviour, or product.

Diffusion of Innovation theory is most suitable to products that possess potential usage in high technology applications (Raeisi & Lingjie, 2016). Rogers (2003) claims that adoption is a decision of “full use of an innovation as the best course of action available” and rejection is a decision “not to adopt an innovation”. This means adoption must be supported by people’s perception of innovation. Malufu, Muchemwa and Malufu (2016) highlight that Diffusion of Innovation is the most acceptable model to describe mobile commerce adoption between different societies and they assert that DOI is a good model to describe user behaviour regarding mobile technology acceptance. Rogers (2003) classifies Diffusion of Innovation into five features of innovation: Compatibility, Complexity, Trialability, Relative Advantage and Observability.

According to Rogers’ (2003) studies, individuals’ perceptions of these features estimate the frequency of adoption of innovations. Some constructs were identified by researchers beyond roger’s classification such as Image, Cost and Voluntariness and also some researchers viz.

Tornatzky and Klein (1982); Moore and Benbasat (1991) extend some constructs for Rogers' (2003) classification.

The innovation process in an organization consists of two main groups of activities (Rogers, 2003): (1) Initiation, consisting of information gathering, conceptualization and planning for the adoption of innovation, decision to adopt, and (2) implementation, consisting of all the events, actions and decisions involved in putting the innovation into use (Abdurachman & Sriwardiningsih, 2016). DOI consists of the following constructs:

(a) Relative Advantage

Rogers (2003) as well as Legg and Mitchell (2016) define Relative Advantage as the degree to which an innovation is perceived as being better than the idea it supersedes. So, the rapid rate of adoption will be perceived relative to the advantage of new products. In the case of mobile commerce, potential to save time is the most visible determinant of Relative Advantage.

(b) Compatibility

Yunus (2014) describes compatibility as the degree to which the new innovation goes along with previously values, attitudes, needs of potential adopters and experiences of using predecessors and the necessity of future adopters.

(c) Complexity

Aizstrauta, Ginters and Eroles (2014) state that Complexity is the degree to which innovation is realized that is very hard to perceive or use. New concepts that are easy with regard to perception are accepting more speedy innovations that need the user to expand understandings.

(d) Trialability

Trialability is the degree to which innovations can be examined on a limited foundation (Degerli, Aytakin & Degerli, 2015). An innovation that is trialable indicates less risk to the individual who is considering it.

(e) Observability

Ndekwa (2015) and Maupa (2014) highlight Observability as the degree to which results of the innovation are tangible to the participant. Sila (2013) claims that the visible results of the

innovation make possible the faster Diffusion of Innovation in the applicable environment and the social system. According to Chen and Wang (2016) as well as Kaleta (2014), only some factors such as Relative Advantages, Complexity and Compatibility of DOI have an important influence on the adoption of innovation of new products or systems and these factors are closely related to the technology acceptance model that follows. The theory can be depicted as shown in figure 2.23.

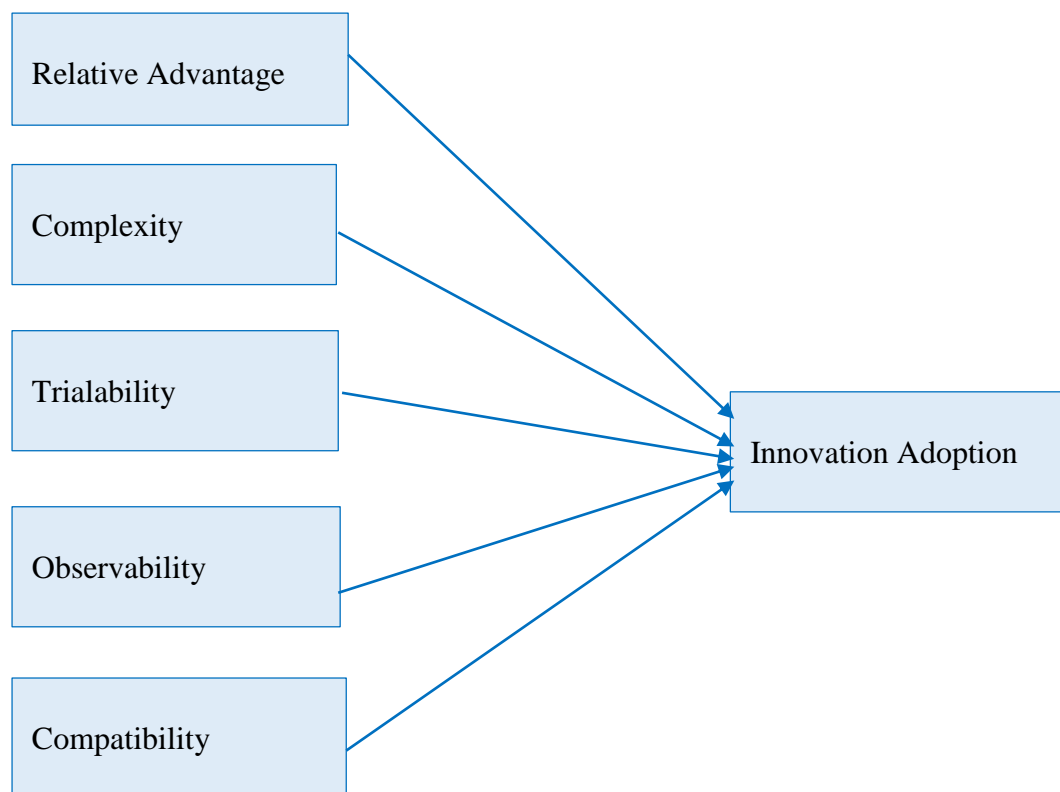


Figure 2.23: Diffusion of Innovation, source: (Rogers, 2003)

2.6.3 TECHNOLOGY ACCEPTANCE MODEL

The Technology Acceptance Model (TAM) was used by many studies to investigate the adoption of new information system/computer usage behaviour, e.g. Abu-Assi, Al-Dmour and Zu'bi (2014), Durodolu (2016), Al-Shbiel and Ahmad (2016), Maduku (2016). TAM is mainly derived from the Theory of Reasoned Action (TRA) that was developed by Fishbein and Ajzen (1975). TAM model incorporates two antecedent variables: “Perceived Usefulness and Perceived Ease of Use”, determining the acceptability of an information system.

The Technology Acceptance Model (TAM) was developed by Fred Davis when working on a contract for IBM Canada in the 1980s. The Technology Acceptance Model (TAM) is developed based on the Theory of Reasoned Action, and it was developed to fit the field of information systems. It was originally specified by Davis Jr (1986) and later refined by Davis and Bagozzi (1989). According to Tang and Hsiao (2016), this theoretical model hypothesized that the actual use of a certain technology is directly influenced by a person's behavioural intention to use, which in turn, is determined by Perceived Usefulness (PU) and Attitude Toward the technology. In addition, users' Perceived Ease of Use (PEOU), another key determinant of TAM, is modelled as the antecedent factor of the PU and Attitude.

TAM is used to understand the variables affecting the degree of internet usage in financial services (Davis & Bagozzi, 1989). According to Rawashdeh (2015), the Perceived Ease of Use and Perceived Web Privacy affect Perceived Usefulness and Behavioural Intention Towards using Internet Banking while Perceived Usefulness, Perceived Ease of Use, and Perceived Web Privacy have a direct and indirect influence on Behavioural Intention.

According to (Erasmus, Rothmann & Van Eeden, (2015), Chen, Chen & Yeh, 2016), TAM theories are that of a technology that is easy to use and if found to be useful will have a positive influence on the intended users' attitude that will increase intentions to use that technology; also TAM applications are mainly focused on the influence of Perceived Usefulness, Perceived Ease of Use, Attitude or Perception towards the use, Behaviour Intention and finally lead to actual usage behaviour. Zogheib and Rabaa'i (2015) state that researchers have found that the original TAM variables might not adequately capture key beliefs that will influence consumers' attitudes towards e-commerce. As a result, TAM has been revised in many studies to fit a particular context of technology being investigated. One important and well-received revision of TAM has been the inclusion of social influence processes in predicting the usage behaviour of a new technology by its users (Venkatesh & Davis, 2000).

TAM addresses the issues of users' attitude towards use of technology and its actual usage. TAM suggests that when users are presented with a new technology, a number of factors determine their decision about how and when they will use it (Ahlan & Ahmad, 2015). According to Alsamydai (2014), many researchers have studied the relationship between perceived ease of use and perceived usefulness. Perceived Usefulness can be defined as the prospective user's subjective probability that using a specific application system will enhance his or her job or life performance.

Alsamydai (2014) affirms that Perceived Usefulness refers to the extent to which an individual believes that he or she would benefit from using new technology. Perceived Usefulness has been found to directly influence Behavioural Intention, which leads to consumers' actual reaction to the use of the system. If the consumer perceives the product or system useful as usual and satisfying to use, they are likely to decide to accept the system. It is regarded as deciding on the extent to which a person believes that using a particular system will enhance his/her performance (Davis & Bagozzi, 1989).

According to Chen, Chen and Yeh (2016), Sharma (2016), Perceived Ease of Use refers to the degree to which a person believes that using a particular system would be free of mental effort. Based on extensive literature studies done over the past years, it has also been found that Perceived Ease of Use has a significant effect on consumers' intention to use a system or product, either directly or indirectly, and a substantial influence on Perceived Usefulness and Behavioural Intention (Davis & Bagozzi, 1989; Venkatesh & Davis, 2000).

However, it has also been found that Perceived Ease of Use in TAM remains controversial. Some researchers Perceive Ease of Use to directly affect either self-reported use or intended Information Technology use, whereas other literature has not found a direct link between Perceived Ease of Use and Information Technology adoption. Sharma and Mishra (2014) state that TAM has been successfully used and adopted by many researchers to study the adoption and acceptance level of the internet-related technologies such as e-mails and m-banking, an example is a study exploring the adoption of internet banking in using TAM. The construct of the Technology Acceptance Model is depicted in Figure 2.24

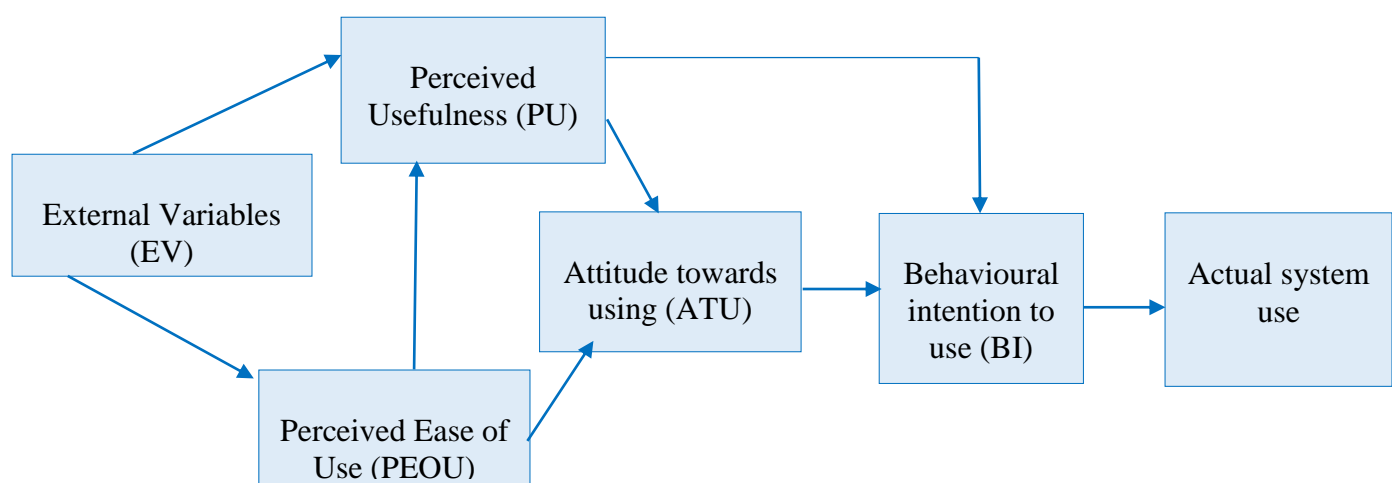


Figure 2.24: Technology Acceptance Model (TAM), source: (Davis, 1989)

2.6.4 TECHNOLOGY ACCEPTANCE MODEL 2 (TAM 2)

In 2000, Technology Acceptance Model (TAM2) as depicted in figure 2.25 was developed by Venkatesh and Davis (2000) on the basis of TAM. Two processes viz. the social influence processes (Subjective Norm, Voluntariness and Image) and the cognitive instrumental processes (Job Relevance, Output Quality, Results Demonstrability and Perceived Usefulness) were integrated into this model. The two processes were considered to be crucial to the study of user acceptance.

According to Osubor and Chiemeké (2015), TAM2 reflects the impacts of Subjective Norm, Voluntariness and Image. The relationship among the three constructs is an important factor that affects user acceptance or rejection of an innovative system. TAM 2 proposes that subjective norm is the medium of social influence processes; it is defined as a person's perception that most people who are important to him think he should or should not perform the behaviour in question.

In the study conducted by Venkatesh and Davis (2000) it shows that Subjective norm that usages of innovative systems should be differentiated. Thus, Voluntariness was proposed to distinguish usage contexts into mandatory and voluntary settings. In TAM2, Voluntariness is set as a moderating variable and defined as the extent to which potential adopters perceive the adoption decision to be non-mandatory. According to Mutlu and Efeoglu (2013), Image refers to the belief of a group important to an individual that a certain behaviour should be implemented and the implementation of this behaviour by the individual can persistently enhance the quality of internal works of the organization.

According to Wingo, Ivankova and Moss (2017), **job relevance** is a key component of the matching process in which a potential user judges the effects of using a particular system on his/her job. In TAM2 it is defined as an individual's perception regarding the degree to which the target system is applicable to his/her job (Sargolzaei, 2017). Leyton, Pino and Ochoa (2015) define **output quality** as the degree to which an individual judges the effect of a new system. In other words it is the degree to which one thinks that a new system can perform required tasks. TAM2 theorizes that **result demonstrability** defined by Moore and Benbasat (1991) as the tangibility of the results of using the innovation will directly influence perceived usefulness. This implies that users will have more positive perceptions of the usefulness of a system if positive results are readily discernible.

TAM2 theorizes that users' mental assessment of the match between important goals at work and the consequences of performing job tasks using the system serves as a basis for forming perceptions

regarding the usefulness of the system (Lai, 2017). The results revealed that TAM2 performed well on both voluntary and mandatory environment.

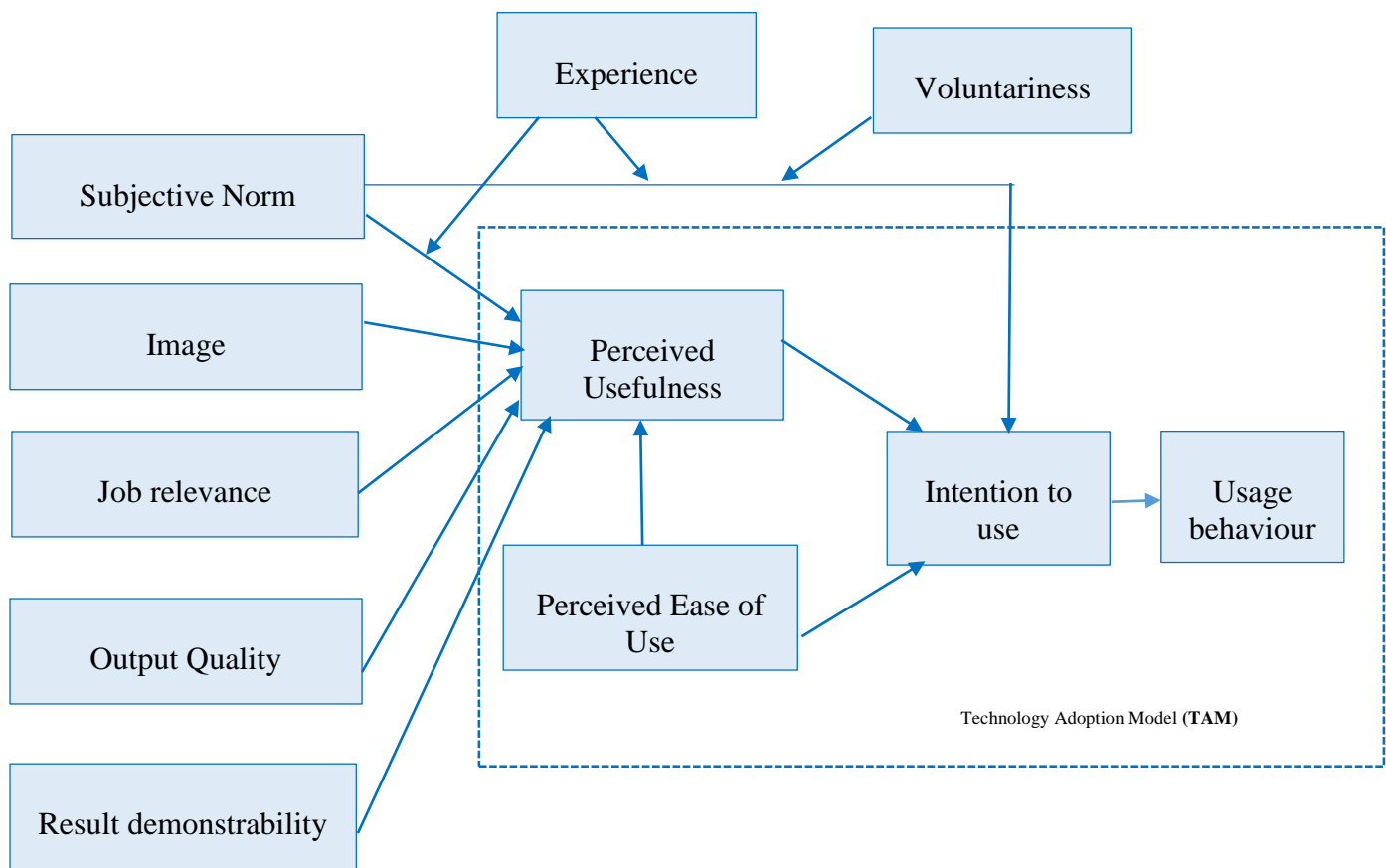


Figure 2.25: Technology Acceptance Model 2(TAM2), source: (Venkatesh & Davis, 2000)

2.6.5 TECHNOLOGY ACCEPTANCE MODEL 3 (TAM3)

Venkatesh and Bala (2008) combined TAM2 (Venkatesh & Davis, 2000) and developed the TAM3 to give a higher level of significance to Perceived Ease of Use. They also added the dimensions of computer Self-Efficacy, Perception of External Control, Computer Anxiety and Computer Playfulness. Two adjustment variables have also been added, viz. Perceived Enjoyment and Objective Usability. TAM3 is constructed on a theoretical framework of four classifications which Venkatesh and Bala (2008) claim is a synthesis of all prior TAM research. These four classifications are individual differences, system characteristics, social influence and facilitating conditions (Alomary & Woollard, 2015).

According to TAM3 model, the Perceived Ease of Use is determined by Computer Self-Efficacy, Computer Playfulness, Computer Anxiety, and Perception of External Control,

Perceived Enjoyment and Objective Usability (Jeffrey, 2015). The Perceived Usefulness is determined by Subjective Norm, Job Relevance, Result Demonstrability and Image (Ahlan & Ahmad, 2015). However, one of the criticisms of the model is that there are too many variables and too many relationships between the variables. Ming-Chih, Shih-Shiunn, Hung-Ming and Wei-Guang (2016) indicate that in TAM3 research model, the Perceived Ease of Use to Behavioral Intention was moderated by experiences. The TAM3 research model was tested in real world settings of IT implementations. See Figure 2.26 for Technology Acceptance Model 3 (TAM3).

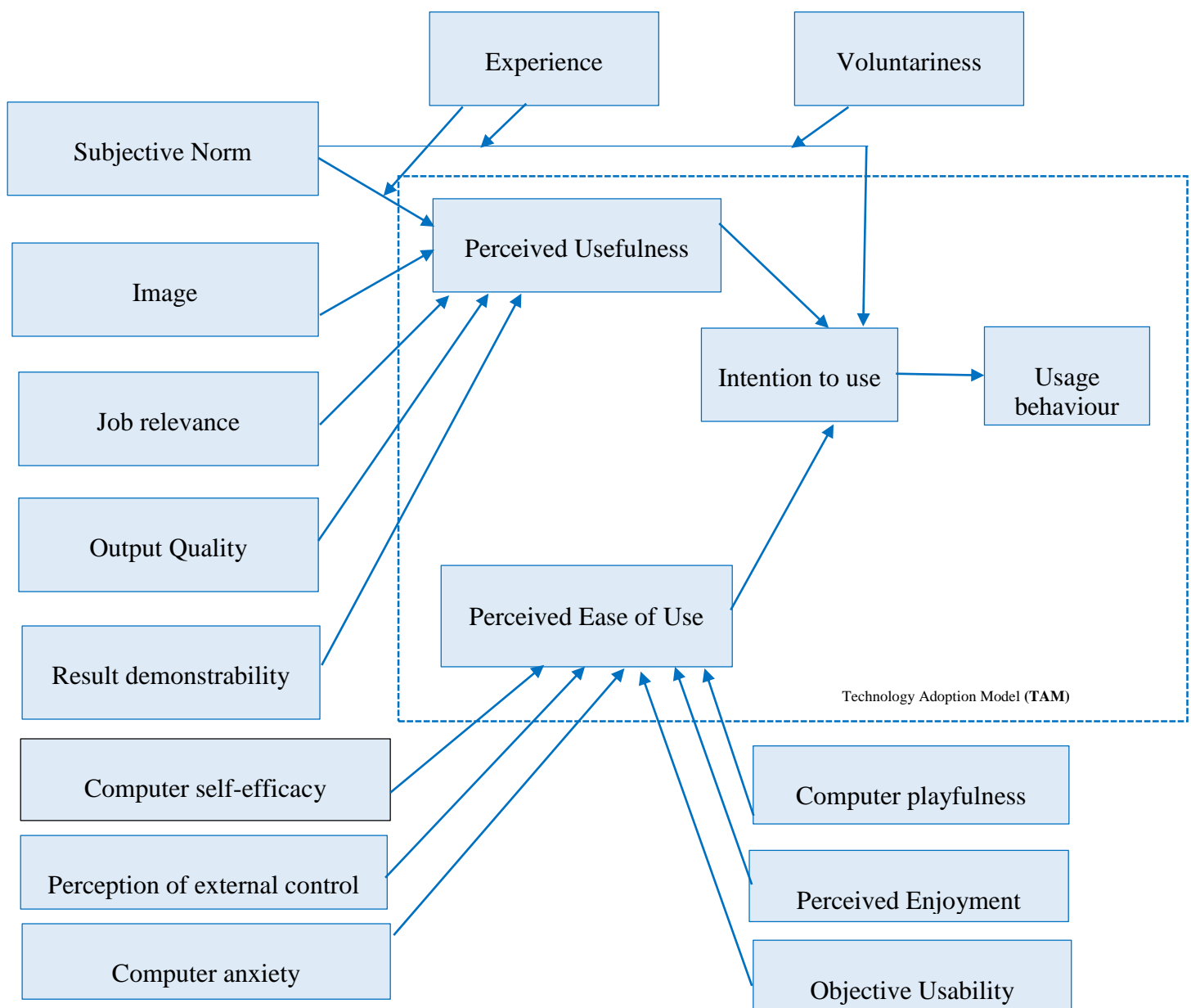


Figure 2.26: Technology Acceptance Model 3 (TAM3), source (Venkatesh & Bala, 2008)

2.6.6 THEORY OF PLANNED BEHAVIOUR (TPB)

Theory of Planned Behaviour (TPB) proposed by Ajzen (1985) has been widely used in research that related to behaviour. TPB examines the relationship between the intention and the actual behaviour with the understanding that any person's behaviour is dependent on the person's volitional control or activities plan. According to the theory of Ahmad, Tarmidi, Raidzwan, Hamid and Roni (2014), there are three major determinants of intention, which are Attitude Towards the Behaviour, Subjective Norm and the Perceived Behavioural Control.

Wang, Li, Zhang and Li (2016) describe Attitudes Towards Behaviour as the individual's positive or negative evaluation of performing the behaviour while Subjective Norm are reflecting with the Social Influence. It is described as the person's perception of the social pressure put on him or her to perform or not to perform the behaviour. They will have a stronger intention towards performing the behaviour if they think they will receive positive feedback and attention from others from doing so (Kim-soon, Ahmad & Ibrahim, 2016). According to Fichten et al. (2016), TPB is a general model to predict behaviour that states that intention is an indication of a person's readiness to perform a given behaviour and it is considered to be the immediate antecedent of behaviour. Generally, the stronger the intention to engage in behaviour, the more likely should be its performance. Furthermore, Perceived Behavioural Control and Attitudes influence intention directly (Stranieri, Ricci & Banterle, 2016). The construct of Theory of Planned Behaviour is depicted in Figure 2.27.

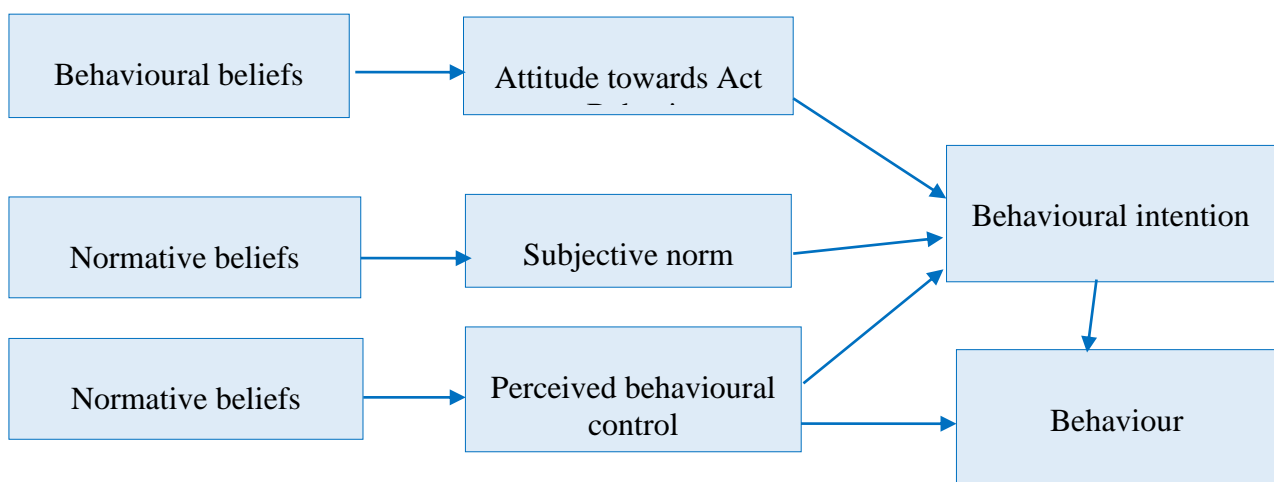


Figure 2.27: Theory of Planned Behaviour, source (Ajzen, 1985)

2.6.7 UNIFIED THEORY OF ACCEPTANCE AND USE OF TECHNOLOGY (UTAUT)

Unified Theory of Acceptance and Use of Technology (UTAUT) is proposed by Venkatesh, Morris, Davis and Davis (2003). The model integrates significant rudiments across eight prominent user acceptance models and formulates a unique measure with core determinants of User Behavioural Intention and Usage. It is the most widely used model to explain an individual's acceptance of an information system. UTAUT has four key constructs: Performance Expectancy, Effort Expectancy, Social Influence, and Facilitating Conditions that influence Behavioural Intention to use a technology and/or technology use (Venkatesh, Thong & Xu, 2016). According to UTAUT, Performance Expectancy, Effort Expectancy and Social Influence are theorized to influence Behavioural Intention to use a technology, while Behavioural Intention and facilitating conditions determine technology use (Yaser, Slewa-Younan, Smith, Olson, Guajardo & Mond, 2016).

According to Raeisi and Behboudi (2016), the first of the four constructs viz. **performance expectancy**, is the degree to which an individual believes that using the system will help him or her to attain gains in job performance. Performance expectancy is the strongest predictor of user intention. The construct is moderated by gender and age and it depicts that men and especially younger men have more intense effect. Kolog, Sutinen, Vanhalakka-ruoho, Suhonen and Anohah (2015) define **effort expectancy** as the degree of simplicity associated with the use of a particular system, whereas **social influence** is referred to as the degree to which an individual perceives that important others believe he or she could use the particular system (Abrahamo, Moriguchi, Naomi & Andrade, 2016). **Facilitation condition** is the degree to which an individual believes that an organizational and technical infrastructure exists to support the use a particular system (Venkatesh, Morris, Davis & Davis, 2003). The construct holds that an individual is influenced by the way she thinks others will view her having used the particular technology.

According to Alwahaishi and Snásel (2013), performance expectancy reflects the perceived utility associated with using mobile internet. Extant research has also noted the effect of Perceived Usefulness (similar to performance expectancy) on satisfaction. Williams, Rana and Dwivedi (2015) indicate that in the past years since the introduction of UTAUT it has been widely employed in technology adoption and diffusion research as a theoretical lens by researchers conducting empirical studies of user intention and behaviour. Al-mamary, Al-

Nashmi and Hassan (2016), as well as Ahmad, Tarmidi, Raidzwan, Hamid and Roni (2014) remark that UTAUT has been discussed with reference to a range of technologies including the internet, web sites, mobile technology among others, with different control factors such as age, gender, experience and education and also focusing upon a variety of user groups.

In a work with academics, Oye, Iahad and Rahim (2014) show the relevance of UTAUT in anticipation of acceptance and use of information and communication technologies by the staff of a University of Nigeria (ADSU – Adamawa State University). The case studied showed the intention to use technologies that are easy to use and promote better professional performance. The results highlighted the Expectation of Effort and Social Influence as the main predictors and put Time and Technical Support as the main barriers to the acceptance and use of technology. In another work Martins, Oliveira and Popovic (2014) developed a conceptual model that combines the Unified Theory of Acceptance and Use of Technology (UTAUT) with the Perceived Risk to explain Behavioural Intention and Internet Banking Use Behavior. The survey was conducted with students and former students of a Portuguese University and concluded about the importance of the Performance Expectation, Effort Expectation, Social Influence and Risk Factors in the prediction of Intention. The construct of the Unified Theory of Acceptance and Use of Technology is depicted in Figure 2.28.

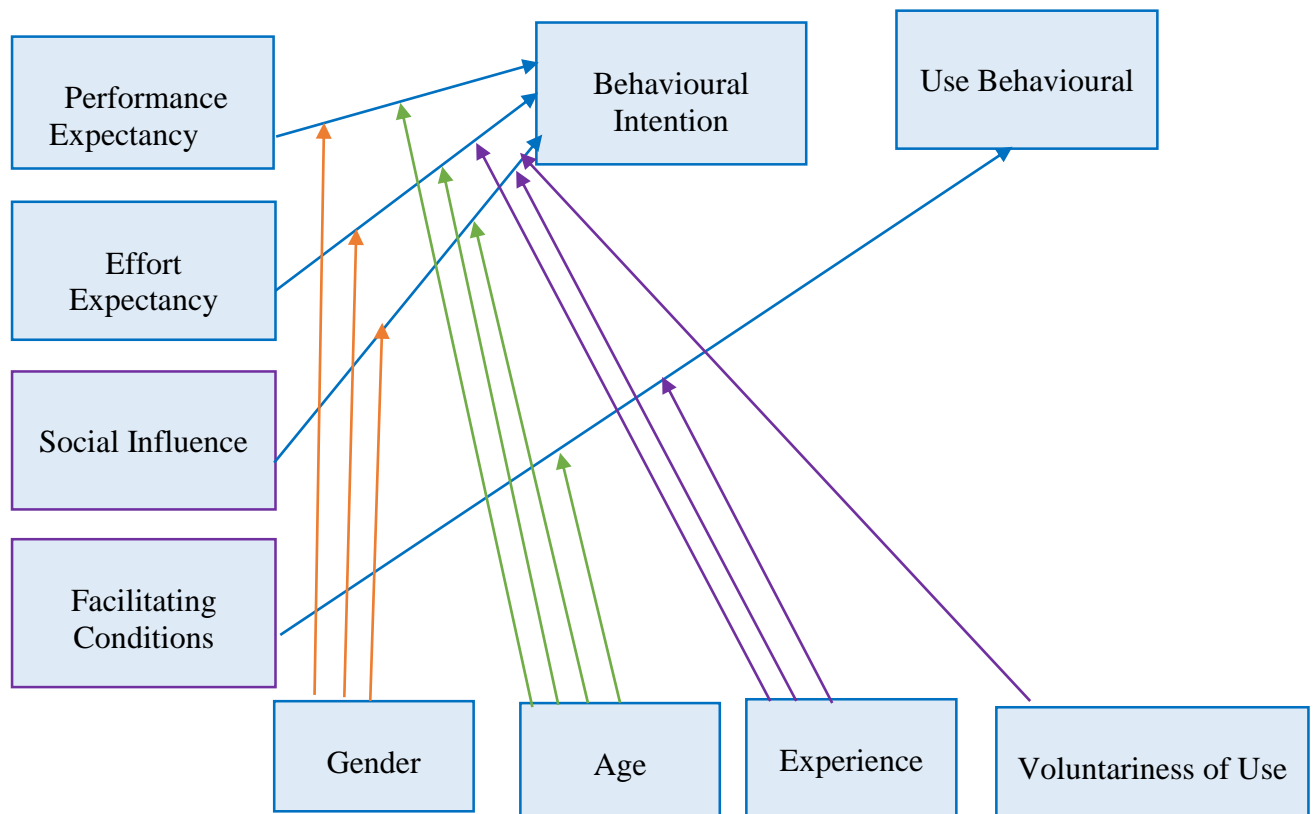


Figure 2.28: Unified Theory of Acceptance and Use of Technology (UTAUT), source (Venkatesh, Morris, Davis & Davis, 2003)

2.6.8 TECHNOLOGY-ORGANIZATION-ENVIRONMENT MODEL (TOE)

Technology-Organization-Environment Model (TOE) was developed by Tornatzky et al. (1990) as an application level model for research from the organization-level perspective (Piaralal, Nair, Yahya & Karim, 2015). TOE model proposes three main facets to explore the factors that affect the organization's acceptance of innovation technology. The Technological Context includes the characteristics and the usefulness of the innovative technology; the Organization Context contains the internal issues within the company such as management, employee, products and services; and the Environmental Context involves the issues existing in the business related field, such as the competitors and business partners (Rahayu & Day, 2015). Micheni (2015) indicates that the TOE model was proven to be fairly effective from the past research. A lot of studies about innovation technologies have been done by adopting the TOE research method, including information systems (Tornatzky, Fleischer & Chakrabarti , 1990), e-commerce (Maarop & Omar, 2015), web

service (Gangwar, Date & Ramaswamy , 2015) and cloud computing (Jiunn-Woei & Yen, 2014).

The Technology-Organization-Environment (TOE) model of Tornatzky, Fleischer and Chakrabarti, (1990) assumes a generic set of factors to predict the likelihood of electronic commerce adoption. The theory suggests that adoption is influenced by technology development. Organizational conditions, business and organizational reconfiguration (Chui-Yu, Chen & Chun-Liang, 2017), and industry environment (Leung, Fong & Law , 2015). Technological Context describes that adoption depends on the pool of technologies inside and outside the firm as well as the application's Perceived Relative Advantage (gains), Compatibility (both technical and organizational), Complexity (learning curve), Trialability (pilot test/experimentation), and Observability (visibility/imagination).

According to Hoti (2015), Organizational Context captures a firm's business scope, top management support, organizational culture, complexity of managerial structure measured in terms of centralization, formalization, and vertical differentiation, the quality of human resource, and size and size related issues such as internal slack resources and specialization (Yi-Shun, Hsien-Ta, Ci-Rong & Ding-Zhong, (2016) Tornatzky, Fleischer & Chakrabarti, 1990).

Environmental Context relates to facilitating and inhibiting factors in areas of operations. Significant amongst them are competitive pressure, trading partners' readiness, socio-cultural issues, government encouragement, and technology support infrastructures such as access to quality Information and Communication Technology (ICT) consulting services (Padilla-Vega, Senquiz-Diaz & Ojeda, (2017), Hassan, Mohdnasir, Khairudin & Adon, (2017), Quinting, Lins, Szefer & Sunyaev, 2017). TOE framework underscores (Rogers, 1995) three groups of adoption predictors- leader characteristics relating to change: internal characteristics (centralization, complexity, formalization, interconnectedness, organizational slack and size), and external characteristics (system's openness). According to Park, Kim and Paik (2015), the major snag of TOE is that some of the constructs in the adoption predictors are assumed to apply more too large organizations, where clients are sure of continuity and fewer complaints, than to Small and Medium-sized Enterprises (SMEs). However, integrating TOE with other models such as TAM, with each adoption predictor offering a larger number of constructs than the original, provides richer theoretical lenses to the understanding of adoption behaviour

(Angeles, 2014). The construct of Technology-Organization-Environment model is depicted in Figure 2.29.

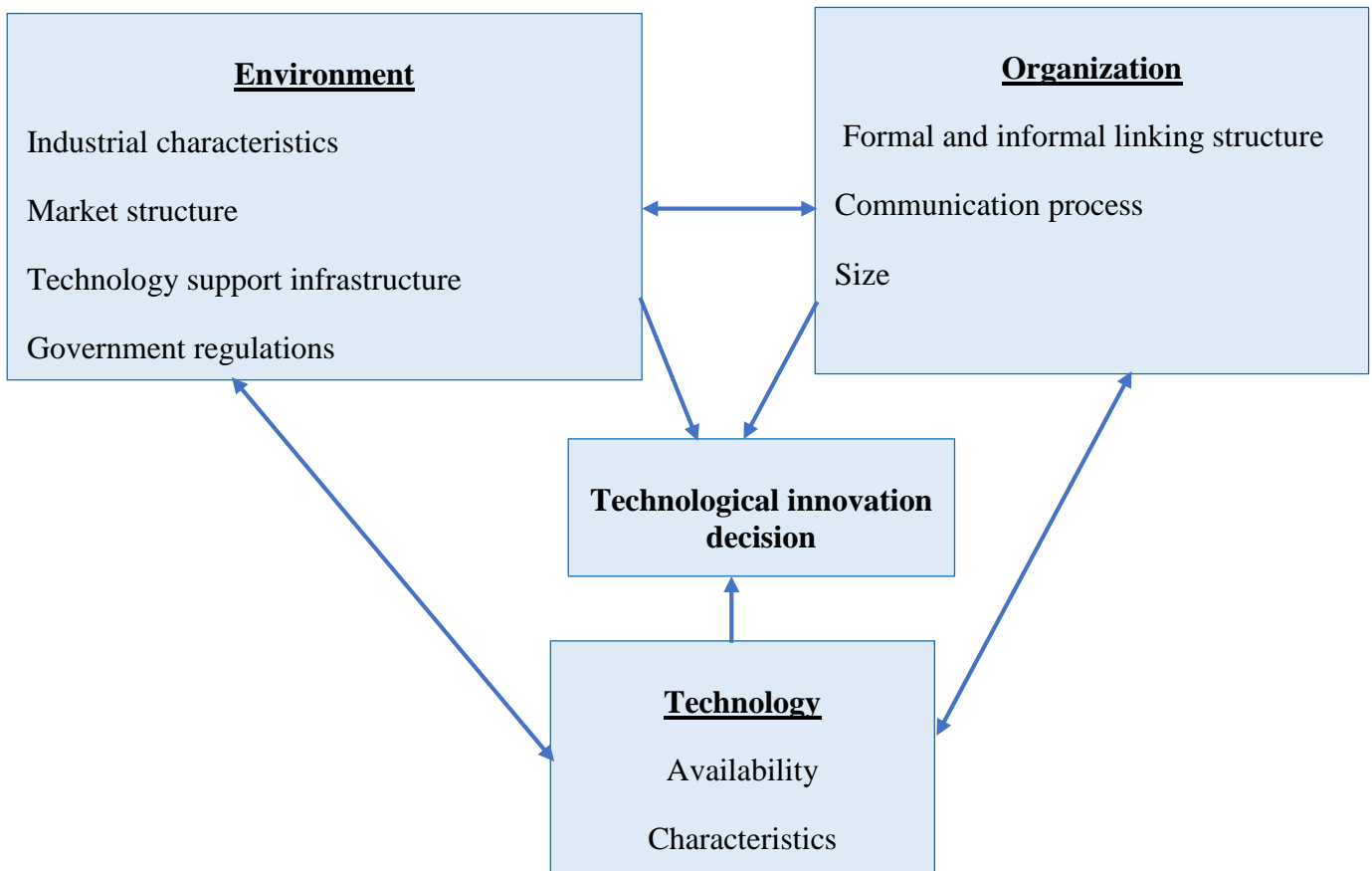


Figure 2.29: Technology-Organization-Environment Model, source (Tornatzky, Fleischer & Chakrabarti, 1990)

2.7 SUMMARY OF TECHNOLOGY ADOPTION MODELS

Table 2.1: Technology Adoption Models Summary (researcher)

| Summary of Technology Adoption Theories | | | |
|---|---|---|---|
| Authors | Factors | Adoption Model | Findings |
| 1. (Nyeko & Ogenmungu, 2017) | Relative Advantage Complexity, Compatibility, Size, IS/IT knowledge, Top Management Support, Competition Pressure, Regulatory Environment, E-learning Adoption | Technology-Organization-Environment (TOE) | Relative Advantage, Complexity with p value of 0.000 are significant predictor of e-learning adoption. Compatibility, Size, Competitive Intensity and Regulatory Environment with p value less than 0.05 are significant predictors of e-learning adoption. IS/IT knowledge, Top Management Support are not significant predictors of e-learning adoption with p value greater than 0.05. |
| 2. (Alwan & Al-Zu'bi, 2016b) | Privacy and Security, Perceived Usefulness, Perceived Ease of Use, Web Service Quality, Customer Trust, Customer Feedback | Technology Acceptance Model (TAM) | Privacy and Security, Perceived Usefulness, Perceived Ease of Use, Customer Trust, Web Service Quality with the standardised coefficient (Beta) values positive and significant at the confidence level $p \leq 0.05$. Customer feedback has negative association to Internet Banking adoption. |

| | | | |
|-----------------------------------|---|--|---|
| 3. (De Veer et al., 2015) | Age, sex, Educational Level, Performance Expectancy, Social Influence, Self-Efficacy, Intention to Use E-Health | Unified Theory Acceptance and Use of Technology (UTAUT) | Correlations between Intention to Use, Performance Expectancy, Social Influence and Self-Efficacy were moderately strong (all pearson r values between .36 and .69, $p < .001$) except for the correlations of Social Influence with Intention to Use ($r = .25$, $p < .001$) and with Self-Efficacy ($r = .17$, $p < .001$). Self-Efficacy was related most strongly to Effort Expectancy ($r = .62$). |
| 4. (Olasina, 2015) | Gender, Customer Services, Type of Bank, Perceived Usefulness, Perceived Ease of Use, Social Influence, Behavioural Intention, ICT skills | Unified Theory Acceptance and Use of Technology (UTAUT) | The results of the relationships between factors such as Customer Services, type of Bank, Perceived Usefulness and Perceived Ease of Use and the Use of m-banking by academics in Nigeria revealed that Customer Services ($r = 0.021$), Perceived Usefulness ($r = 0.041$), Perceived Ease of Use ($r = 0.097$) and Social Influence ($r = 0.049$), were positively correlated with the Use of m-banking by academics. However, the type of bank ($r = -0.051$) and Gender ($r = -0.107$) were found to be negatively correlated with the use of m-banking by the academics. Behavioural Intention ($r = 0.172$) and ICT skills ($r = 0.104$) were positively correlated with the Use of m-banking by the academics. |
| 5. (Wingo, Ivankova & Moss, 2017) | Technology Acceptance Model 2 (TAM2) | Experience, Image, Job Relevance, Output Quality, Result Demonstrability, Voluntariness, Behaviour Usage, Intention to use, Subjective Norm, | Studies in this review revealed concerns among faculty regarding their perceived barriers to student success in online classes, uncertainty about their image as online instructors, technical support needs, and their desire for reasonable workload and manageable class enrolments in online classes. |

| | | | |
|--|--------------------------------------|---|---|
| | | Perceived Usefulness, Perceived Ease of Use. | |
| 6. (Mutlu & Efeoglu, 2013) | Technology Acceptance Model 2 (TAM2) | Subjective Norm, E-mail Usage, Behavioural Intention, Perceived Usefulness, Collectivism, Femininity | Perceived Usefulness and Perceived Ease Of Use have positive effects on Behavioural Intention, Perceived Ease Of Use and Subjective Norm both effect Perceived Usefulness, Femininity shows positive moderating effect on the relationship between Subjective Norm and Perceived Usefulness as well as the relation between Subjective Norm and Behavioural Intention, Collectivism shows positive moderation effect between Subjective Norm and Perceived Use, moderation effect of Subjective Norm on Perceived Usefulness is higher for people who have higher tolerance to uncertainty. |
| 7. (Ming-chih, Shih-shiunn, Hung-ming & Wei-guang, 2016) | Technology Acceptance Model3 (TAM3) | Voluntariness, Experience, Subjective Norm, Image, Perceived Usefulness, Usage Behaviour, Job Relevance, Intention to Use, Output Quality, Perceived Ease of Use, Result Demonstrability, Computer Self-Efficacy, Computer Playfulness, Perception of External Control, Perceived Enjoyment, Computer Anxiety, Objective Usability. | Study result found that Taiwan finance customers had high expectations of information security and preferred high technology products with complex functions. The result demonstrated that Customer's Use Behaviour was influenced by Perceived of Usefulness, not Perceived of Ease of Use. The moderator effect result in Experience had a positive moderator effect on Objective Usability to Perceived Ease of Use. |

| | | | |
|-----------------------------------|--|--|--|
| | | | |
| 8. (Shatat, 2017) | Technology Acceptance Model (TAM) and Theory of Reasoned Action (TRA) | Privacy, Lack of Awareness, Perceived Ease of Use, Usefulness, Cultural, Social Issues, Security, Trustworthiness, Intention to Adopt, Adoption and Usage of Online Services | Usefulness, ease of use, security, Awareness, Trustworthiness and Privacy are significantly and positively correlated with the Adoption and Usage of Online Services. Cultural and Social Issues show no contribution at all to the overall adoption of online services. |
| 9. (Ramavhona & Mokwena, 2016) | Diffusion of Innovation theory (DOI) | Awareness, Relative Advantage, Compatibility, Complexity, Trialability, Security | Compatibility, Trialability and external variables such as Awareness and Security were found to have significant influence in the adoption of internet banking in South African rural areas, whereas Relative Advantage was found not to be a significant factor. Security and Complexity of the internet banking were also revealed as some of the factors hampering the intention to adopt internet banking. |
| 10. (Santouridis & Kyritsi, 2014) | Web Usage Intensity Domain Personal Innovativeness prior E-shopping Experience, Satisfaction with: Traditional Bank Branches | Technology Adoption Model (TAM) | Perceived Usefulness (.347), Domain Personal Innovativeness (.297), Perceived Credibility (.214), Satisfaction with ATMS (.160), Perceived Ease of Use (.123) have a significant positive effect on Behavioural Intentions, while increasing income (-.089) affects it negatively. 60.3% of the Behavioural Intentions variance is explained by the independent variables. |

| | | | |
|--------------------------|--|-----------------------------------|--|
| | ATMS, Perceived Usefulness, Perceived Ease of Use, Perceived Credibility, Behavioural Intention | | |
| 11. (Mwiya et al., 2017) | Perceived Usefulness Perceived Ease of Use Perceived Trust Attitude Towards e-banking Intention to adopt e-banking, e-banking adoption | Technology Acceptance Model (TAM) | <p>All variables (Perceived Usefulness, Perceived Ease of Use, Perceived Trust, Attitude Towards e-banking, Intention to adopt e-banking), e-banking adoption has low inter-correlations among each other all of them below 0.80. This entails that multicollinearity is not a problem. Gender and Level of Education are significantly associated with e-banking use Intention and Actual Adoption. Age is insignificant.</p> <p>Attitude Towards e-banking services is positively significantly associated with each independent variable (all sig. <0.01) namely Perceived Usefulness (r=0.622), Perceived Ease of Use (r=0.509) and Perceived Trust (r=0.493)</p> |
| 12. (Ahmed & Phin, 2016) | Internet banking users and non-users Demographic factors Social Influences Adoption of banking | Technology Acceptance Model (TAM) | Usefulness of Internet banking, Ease of Use of internet banking and Risks of Internet banking were most influenced factors. Results show risks of internet banking are negatively related to the adoption of internet banking use. Usefulness and Ease of Use have activist relation with internet banking. |

| | | | |
|--|---|--|---|
| 13. (Soh & Hong, 2014) | Cost Saving, Features Availability, Risk and Privacy, Convenience Adoption of Internet Banking | Uses of Gratifications Model | Cost Saving significantly predicts the adoption of Internet Banking with p value 0.019. Features Availability significantly predicts the adoption of Internet Banking with p value 0.046. Risk and Privacy significant predict the adoption of internet with p value 0.000. Convenience significantly predicts the adoption of Internet Banking with p value 0.000. |
| 14. (Goswami, 2017) | Perceived Ease of Use, Perceived Usefulness, Utilitarian Attitude, Hedonic Attitude, Usage Intention | Extended Technology Acceptance Model (TAM) | Perceived Ease of Use strongly predicted Perceived Usefulness of m-banking applications ($\beta=0.74$, $p<0.01$), Perceived Usefulness predicted strongly Usage Intentions ($\beta=0.58$, $p<0.01$). Perceived Ease of Use related to using intention ($\beta=0.24$, $p<0.05$). Utilitarian ($\beta=0.36$, $p<0.01$) rather than Hedonic Attitude ($\beta=0.07$) predicted Intention to Use m-banking in the future. Perceived Usefulness strongly predicted Utilitarian ($\beta=0.71$, $p<0.01$), Perceived Ease of Use predicts Utilitarian ($\beta=0.32$, $p<0.01$) but not as much as Perceived Usefulness. Hedonic Attitude is predicted by Perceived Usefulness ($\beta=0.46$, $p<0.01$) but not by Perceived Ease of Use ($\beta=0.07$, $p<0.05$). Hedonic Attitude also predicts Utilitarian ($\beta=0.56$, $p<0.01$). |
| 15. (Chui-Yu, Chen & Chun-Liang, 2017) | Technology- Organization- Environment initiation Adoption Implementation | Technology-Organization- Environment (TOE) and Diffusion of Innovation (DOI) | In terms of Technology Context, Relative Advantage and Compatibility showed significant results in line with the research results that rely on communication tools. Trialability has reached a significant level. Organizational Context significantly affects the Adoption of Broadband Mobile Applications |

| | | | |
|---------------------------------|---|---|---|
| | | | Environment context has a significant effect on adoption of broadband mobile applications. |
| 16. (Hussein & Baharudin, 2017) | Financial Support Information Intensity IT Competency Relative Advantage E-Commerce Continuance Intention | Technology-Organization-Environment(TOE) | The results show the positive relationship of IT Competency on E-Commerce continuance intention with $\beta=0.166$ and significant with t-value=3.211 and $p<0.01$. Positive relationship of Relative Advantage of E-Commerce continuance intention with $\beta=0.450$ and significant with t-value=6.812 and $p<0.001$. Financial Support and Information Intensity have no significant relationship with E-Commerce continuance. |
| 17. (Joseph, 2017) | Perceived Usefulness Perceived Ease of Use Attitude Towards Using, Behavioural Intention to Use, Actual System Use External variable | Technology Acceptance Model (TAM) | Perceived Ease of Use and Perceived Usefulness positively contribute to the realization of CU. A regression analysis, predicting log-Perceived Usefulness from Perceived Ease of Use was highly statistically significant with $F(1)=59.702$, $p<.001$. Citizens perceived e-government important as over 75 of the participants are certain that e-government can bring public information closer to the people. |
| 18. (Fathima & Muthumani, 2015) | Perceived Usefulness, Perceived Ease of Use Perceived Credibility | Technology Acceptance Model (TAM) and Unified Theory Acceptance and | All the constructs taken for the study including Perceived Usefulness, Perceived Ease of Use, Perceived Credibility, Trust, Facilitating Conditions, Perceived Cost, Subjective Norm, Image and Self-Efficacy are significant and hence positively influence the Intention |

| | | | |
|--|---|---------------------------|--|
| | Trust Perceived Cost Facilitating Conditions Subjective Norm, Image, Self-Efficacy | Use of Technology (UTAUT) | to Use Internet Banking. Perceived Cost is the least predictor of Intention to Use Internet Banking. |
|--|---|---------------------------|--|

2.8 CHAPTER 2 SUMMARY

In this chapter mobile computing background, its security issues, types of e-applications, benefits and users' perceptions around various e-applications have been discussed. Also, technology adoption models and their summary have been explained in order to be utilized to formulate a research framework in the next chapter. The next chapter will provide an explanation of the approach, method, research design for conducting the research, proposed research model, research hypotheses to be tested and how data was collected and analyzed.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 INTRODUCTION

This chapter represents the research design and research approach including population, sample and sampling method, research instrument, procedure for data collection, data processing and analysis, ethical considerations and study limitation. The chapter contains the approach used to achieve the objectives of the study. It then goes on to discuss the software used to analyse the data reliability, validity, testing of hypothesis based on users' perceptions on security of mobile computing for adoption of e-applications to achieve the objectives of the study (see chapter 1, section 1.5).

3.2 RESEARCH DESIGN

According to Lin (2015), research design is a plan for a study providing the overall framework for collecting data. This study focuses on the users' perceptions on security of mobile computing in South Africa for adoption of e-applications. This study consists of three phases, namely the theoretical phase, portrayal phase and explanatory phase.

3.2.1 THEORETICAL PHASE

In the theoretical phase the research specifically questions what is the opinion of South African residents on security of mobile computing for adoption of e-applications, and the objectives were formulated for the purpose of the study (see chapter 1, section 1.5). The research questions evolved due to the researchers' involvement in the occurrence under investigation. A literature review was conducted to familiarise the researcher with the theory and content literature.

3.2.2 PORTRAYAL PHASE

The portrayal phase involved planning the design. The questionnaire was the main data collection instrument. A field study was conducted with six hundred (600) sample size. The non-probability sampling method was used. Non-probability is defined as a sampling approach in which the chance or probability of each unit to be selected is not known or confirmed (Rahl, 2017).

3.2.3 EXPLANATORY PHASE

The explanatory phase involved data collection, analysis and interpretation. Data collected included quantitative information that was collected using a survey questionnaire. The research

also searched articles to understand the framework of the topic under the study for the purpose of providing a view of reality that is important to respondents.

3.3 RESEARCH APPROACH

According to Choy (2014), the quantitative approach refers to standardised questionnaires that are administered to individuals or households that are identified through various forms of sampling. According to Bwalya and Mutula (2016), if a problem involves identifying factors that influence an outcome, then a quantitative approach is the best. In this study, a quantitative research approach was used and has reduced the measurement to numbers and also enabled generalization when using the method across a large group of individuals.

Bwalya and Mutula (2016) state that quantitative research is helpful in testing and validating theories, testing hypotheses, replication of findings, allows quantitative predictions, are less time consuming and findings are independent of the researcher. In addition, in this study quantitative research approach facilitated numerical data for groups and extents of agreement or disagreement from respondents or participants. It has provided a short time frame for administering the study and it was reliable for critical analysing.

Quantitative research is primarily investigative research. In this study it was used to gain understanding of underlying reasons, opinions and motivations of users' intention to adopt e-applications. It was used to quantify the problem by way of generating numerical data or data that was transformed into useable statistics and to generalize results from a larger population. According to Monfared and Derakhshan (2015) as well as Padgett (2016), a quantitative data collection method includes different forms of surveys: online surveys, paper surveys, mobile surveys and kiosk surveys.

Quantitative research is substantial and countable in nature and the designs are predetermined and structured, remaining consistent throughout the study; making them potentially reproducible. Leung (2015) indicates that quantitative research deals primarily with numerical data and its statistical interpretations under a reductionist, logical and strictly objective paradigm. In quantitative research it is assumed that cognition and behaviour are highly predictable and explainable (Antwi & Hamza, 2015).

3.4 POPULATION

Choto, Tengeh and Iwu (2014) refer population to any group of individuals that has one or more characteristics in common that are of interest to the research. Furthermore, Antwi and Hamza (2015) define population as a number of people or units from which research information will be obtained. The population of this study is the South African residents who have access to mobile devices.

3.5 SAMPLING SIZE

Sampling size is defined as a technique of electing the number of observations to include in a sample. Additionally, the sample size is an important feature of any study or investigation in which the aim is to make inferences about the population from a sample (Singh & Masuku, 2014). The sample size of this study is six hundred (600).

3.6 SAMPLING METHOD

Sampling process refers to the process of selecting a group of people, events or behaviour with which to conduct a study and it also has advantages of faster data collection and lower cost (Singh & Masuku, 2014). In this study, the non-random sampling was used whereby the researchers used their judgement to select the subjects to be included in the study based on their knowledge of the occurrence. Convenience sampling was used in this study for selecting the participants due to its advantages such as availability of participants, the ease with which participation could be observed and monitored and the quickest way with which the data could be gathered for analysis (Kivunja, 2015).

Kivunja (2015) defines convenience sampling as a type of non-random sampling where members of the target population that meet certain practical criteria such as easy accessibility, geographical proximity, availability at a given time or willingness to participate, are included for the purpose of the study.

3.7 RESEARCH INSTRUMENT

The research instrument used in this study is a survey. According to Ponto (2015) survey research is defined as the collection of information from a sample of individuals through their responses to questions. The survey questionnaire method is regarded as the best method for gathering a large number of responses. Ponto (2015) indicates that this method gathers information about people's attitudes, facts, behaviour, activities and responses to events, and

usually consists of a list of written questions. A brief introduction to the research study was provided to participants before they completed the questionnaire. The researcher used an online based structured questionnaire using a survey monkey and social media to gather information on the respondents' perceptions on the security of mobile computing for adoption of e-applications. The survey questionnaires covered two (2) sections namely:

Section A: Demographic information: This part gathered demographic information such as gender, age, ethnic group, and education level and occupation status. To ensure that honest opinions and answers were obtained, respondents were guaranteed anonymity. Guided questions were used to determine these variables. Respondents chose from a range of questions which ensured that they did not have to disclose specific details that will make them feel uncomfortable.

Section B: Technology Adoption related questionnaires: This section looked into perceptions of respondents towards the intention to adopt e-applications based on Perceived Usefulness of security mechanisms, Perceived Ease of Use of security mechanisms, Subjective norm on security mechanisms, Relative Advantage of security mechanisms, Compatibility of security mechanisms, Aesthetics of security mechanisms and Complexity of security mechanisms. The 5-point Likert scale was used to determine the level of agreement in this regard. A Likert-type scale is usually linked to a number of statements to measure attitudes or perceptions and 5-point or 7-point scales are often used (Sullivan & Artino Jr, 2013; Barua, 2013). The questionnaire in the survey was kept short and standardized, with structured questions in which control or guidance was given.

After reviewing the literature of various prominent Technology Adoption theories, the authors of Technology Adoption theories found two main variables (Perceived Usefulness and Perceived Ease of Use) to be significant direct determinants of technology adoption and use of technology in one or more of the individual models. However, these variables were also used in proposed frameworks. In addition, in this study fieldwork was conducted to produce evidence of Perceived Usefulness of Security Mechanisms and Perceived Ease of Use of Security mechanisms through formulated hypotheses, also the research questionnaire were designed. According to Kinash (2013), fieldwork is a method that the researcher could employ to gather information. The questionnaire used in this research was derived and adopted from the Technology Adoption Model 2 (TAM2) and Diffusion of Innovation (DOI) Model.

However, some modifications have been made to ensure the suitability of questionnaires with the users' perceptions on security of mobile computing for adoption of e-applications.

3.8 PROCEDURE FOR DATA COLLECTION

The data collection method used in this study was survey questionnaire, whereby confidentiality was stressed in all written communications with potential respondents. Respondents' names were not collected with the data. Introductory letters were sent to sampled emails, the social media platform, followed by the link to the survey questionnaire. Through the assistance of friends and family the questionnaire were distributed in a short period of time (4 weeks) i.e. snowball sampling. Email and social media questionnaires are cost saving because there are no travelling costs and print outs needed.

The items used in the survey instrument to measure the constructs were identified and adopted from prior research (Nyeko & Ogenmungu (2017), Erasmus, Rothmann & Van Eeden (2015), Kanwal & Rehman (2014), Chin & Lin (2016), Alsamydai (2014), Sila (2013), Penjor & Zander (2016), Thielsch, Engel & Hirschfeld (2015), Reinecke et al. (2013), Abdekhoda, Dehnad, Mirsaeed & Gavgani (2016), Aboelmged & Gebba (2013), Chen & Wang (2016)), particularly from technology adoption studies, in order to ensure validity of the scale used. The items were widely used in the majority of prior studies indicating potential subjective agreement among researchers that these measuring instruments logically appear to reflect accurate measure of the constructs of interest. Table 3.1 below lists the items developed for each construct in this study as well as sets of prior studies where these items have been adopted from.

Table 3.1: Survey Questionnaire Statements Related to Variables

| Construct | Items | Sources |
|-----------------------------|--|---|
| Demographics Information | User gender, Age, Ethnic Group, Education Level, Occupation Status. | (Nyeko & Ogenmungu, 2017; Erasmus, Rothmann & Van Eeden, 2015) |

| | | |
|--|--|--|
| Perceived Usefulness of security mechanisms | <p>PU1: I find using password/PIN security mechanism on mobile computing useful to access e-applications.</p> <p>PU2: I find using fingerprint security mechanism on mobile computing useful to access e-applications.</p> <p>PU3: I find using a combination of password and finger print security mechanism on mobile computing useful to access e-applications.</p> <p>PU4: I find using pattern security mechanism on mobile computing useful to access e-applications.</p> | (Kanwal & Rehman, 2014; Chin & Lin, 2016; Alsamydai, 2014) |
| Perceived Ease of Use of security mechanisms | <p>PEOU1: I find password/PIN security mechanism easy to use on mobile computing to access e-applications.</p> <p>PEOU2: I find fingerprint security mechanism easy to use on mobile computing to access e-applications</p> <p>PEOU3: I find using combination of password and finger print security mechanism easy to use on mobile computing to access e-applications.</p> <p>PEOU4: I find using pattern security mechanism on mobile computing easy to use to access e-applications.</p> | (Kanwal & Rehman, 2014; Alsamydai, 2014) |

| | | |
|---|--|---|
| Complexity of security mechanisms | <p>COMPL1: Using PIN/Password security mechanism is less complex.</p> <p>COMPL2: Using Fingerprint security mechanism is less complex.</p> <p>COMPL3: Using Pattern security mechanisms is less complex.</p> <p>COMPL4: Using combination of password and finger print security mechanism is less complex.</p> | (Sila, 2013; Penjor & Zander, 2016) |
| Aesthetics of security mechanisms interface | <p>AEST1: Security mechanisms' interface is clearly structured and simple.</p> <p>AEST2: Security mechanisms' interface is beautiful.</p> <p>AEST3: The user interface for security mechanisms' input is designed for all levels of users.</p> <p>AEST4: Security mechanisms' interface is stylish.</p> | <p>(Thielsch, Engel & Hirschfeld, 2015)</p> <p>(Reinecke et al., 2013)</p> |
| Subjective norm on security mechanisms | <p>SN1: Individuals who influence me think that I should use password/PIN security mechanism on mobile computing to access e-applications.</p> <p>SN2: Individuals who influence me think that I should use fingerprint security mechanism on mobile computing to access e-applications.</p> | (Abdekhoda, Dehnad, Mirsaeed & Gavvani, 2016; Kanwal & Rehman, 2014; Alsamydai, 2014) |

| | | |
|---|---|--|
| | SN3: Individuals who influence me think that I should use pattern security mechanism on mobile computing to access e-applications. | |
| Relative Advantage of security mechanisms | <p>RAD1: PIN/Password has more advantages which makes the security more efficient.</p> <p>RAD2: Fingerprint has more advantages that makes the security more efficient.</p> <p>RAD3: Pattern has more advantages that makes the security more efficient.</p> <p>RAD4: Combination of PIN and Fingerprint has more advantages which makes the security more efficient.</p> | <p>(Chen & Wang, 2016)</p> <p>(Penjor & Zander, 2016)</p> |
| Intention to Adopt e-applications | <p>ITA1: I intend to use the e-applications frequently in my life.</p> <p>ITA2: I intend to use e-applications platform as soon as possible.</p> <p>ITA3: I plan to use the e-applications platform in the future.</p> <p>ITA4: I will recommend e-applications to others.</p> | <p>(Al-Ghaith, 2015; Abdekhoda, Dehnad, Mirsaeed & Gavgani, 2016; Aboelmged & Gebba, 2013)</p> |
| Compatibility of security mechanisms | COM1: The function of PIN/password is compatible for e-applications on mobile device. | <p>(Chen & Wang, 2016; Penjor & Zander, 2016)</p> |

| | | |
|--|---|--|
| | <p>COM2: The function of fingerprint is compatible for e-applications on mobile device.</p> <p>COM3: The function of Pattern is compatible for e-applications on mobile device.</p> | |
|--|---|--|

3.8.1 VARIABLES AND OPERATIONAL DEFINITIONS

Table 3.2: Study Variables and Operational Definitions

| Variable | Operational definition |
|--|--|
| Perceived Usefulness of security mechanisms | The extent to which users believe that the usefulness of security mechanisms on mobile devices will enhance the adoption e-applications. |
| Perceived Ease of Use of security mechanisms | The extent to which users believe that the security mechanisms on mobile devices will be easy to use for adoption of e-applications. |
| Aesthetics of security mechanisms interface. | The extent to which users believe that the beauty and the appeal of security mechanisms interface on mobile devices will enhance the adoption of e-applications. |
| Intention to Adopt e-applications | The extent to which users intend to participate in the adoption of e-applications. |
| Compatibility of security mechanisms | The extent to which users believe that the compatibility of security mechanisms on mobile devices will enhance the adoption of e-applications. |

| | |
|---|--|
| Complexity of security mechanisms | The extent to which users believe that the complexity of security mechanisms on mobile devices will hinder the adoption of e-applications. |
| Relative Advantage of security mechanisms | The extent to which users believe that the relative advantage of security mechanisms will enhance the adoption of e-applications. |
| Subjective norm on security mechanisms | The extent to which users believe that the social pressure to use security mechanisms will enhance the adoption of e-applications. |

3.8.2 PROPOSED RESEARCH MODEL

In the research literature review is indicated that users are skilled with various e-applications; when security mechanisms are added into the applications, what are the factors that will lead to users' perceived usefulness of security mechanisms, perceived ease of use of security mechanisms and intention to adopt e-applications? Four factors are chosen from the Diffusion of Innovation theory (DOI) to apply in this research, and also the subjective norm from Technology Adoption Model 2 (TAM2). Previous research of Diffusion of Innovation theory (Azeta & Ibukun, 2016; Penjor & Zander, 2016; Thomas, 2014; Chen & Wang, 2016) applied in the field of information systems show that relative advantage, compatibility and complexity are the most important factors influencing innovation adoption.

The research model used in this study was derived and adopted from the Technology Adoption Model 2 (TAM2) and Diffusion of Innovation theory (DOI) as proposed by Rogers (2003) and Venkatesh and Davis (2000). See figure 3.1 below.

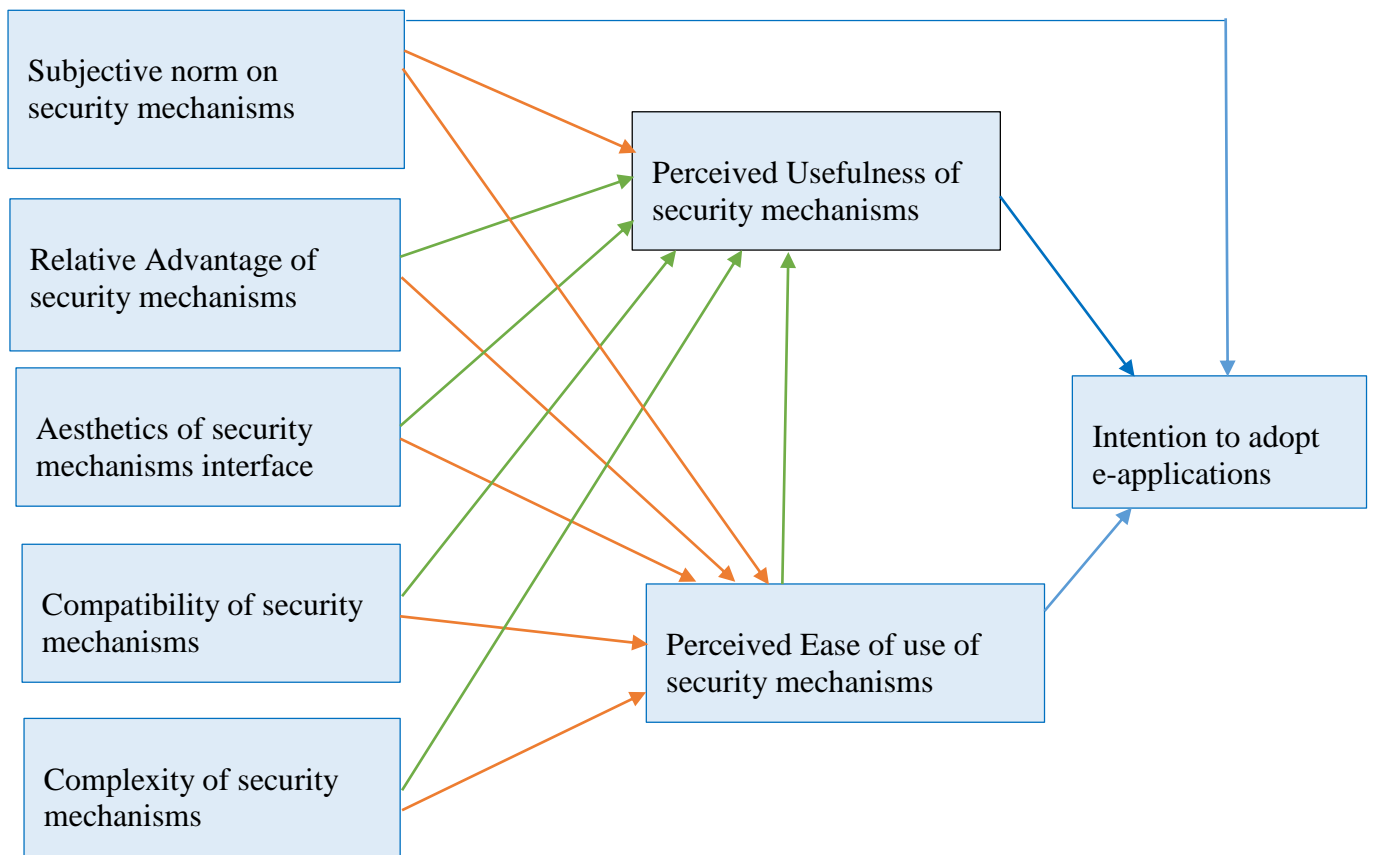


Figure 3.1: Proposed Research Model

3.9 ETHICAL CONSIDERATION

This relates to moral standards that the researcher should consider in all research methods in all research stages. After approval from Vaal University of Technology was obtained to conduct the study, permission was obtained from the Ethics Committee of the Higher Degree office. Therefore, ethical considerations have been adhered to while conducting this study and the following are employed in this study:

All participants willingly volunteered to participate in this study. In terms of confidentiality, all the information discovered in this study was treated confidentially to ensure comfortability for all the participants. With regards to privacy and anonymity, all information provided by the participants was kept private to ensure that readers are unable to identify the participants in the study. The Excel spread sheet that contained participants' data and information was password protected in order to prevent unauthorized people from accessing the data. Informed consent letters were provided to participants, all the participants were aware of the objectives and aim of the study, to ensure that they have an understanding of the outcomes of the study.

3.10 DATA PROCESSING AND ANALYSIS

Data was captured in Excel and exported to IBM SPSS version 24.0 for analysis. The response rate was analysed to calculate the number of surveys distributed, number of surveys completed, and number of surveys filled out. This was followed by the internal consistency between the constructs of the study (reliability test) and the validity test to determine if the research instrument (survey) is truly measuring what it is intended to measure, this include the Kaiser-Meyer-Olkin (KMO), Bartlett's Test of Sphericity and Principal Component Analysis (PCA) using varimax rotation. Furthermore, frequencies and percentages of the demographic information results (section A of questionnaire) and technology adoption related questions results (section B of questionnaires) were also presented using tables. To ensure for technology adoption related questionnaire (section B of questionnaire) consistency, the Cronbach's Alpha (α) was analysed to ensure that the constructs are measuring the same thing.

According to Vaske, Beaman and Sponarski (2017), Alpha was developed by Lee Cronbach in 1951 to provide a measure of the internal consistency of a test or scale. It is expressed as a number between 0 and 1. In addition, internal consistency describes the extent to which all the items in a test measure the same concept or construct and hence it is connected to the inter-relatedness of the items within the test. Internal consistency is concerned with the interrelatedness of a sample of test items. Therefore, the number of test items, item inter-correlations affect the value of alpha.

Furthermore, Vaske, Beaman and Sponarski (2017) state that there are different reports about the good values of alpha, ranging from 0.70 to 0.90. A low value of alpha could be due to a low number of questions, poor inter-correlations between items. Also if alpha is too high it may suggest that some items are redundant as they are testing the same question but in a different appearance (Taber, 2017).

In addition, Cronbach's alpha is considered an adequate measure of internal consistency. A low Cronbach's alpha indicates a lack of correlation between the items in a scale, which makes summarizing the items unjustified (BrckaLorenz, Chiang & Nelson, 2013). Hence, a very high Cronbach's alpha indicates high correlations among the items in the scale, i.e., redundancy of one or more items and a very high Cronbach's alpha is usually found for scales with a large number of items, because Cronbach's alpha is dependent upon the number of items in a scale.

Note that Cronbach's alpha gives no information on the number of subscales in a questionnaire, because alpha can be high when two or more subscales with high alphas are combined.

According to Sharma (2016) Cronbach's Alpha (α) efficient is one of the most commonly used measures of reliability in social science studies. Furthermore, a commonly accepted rule of thumb for describing internal consistency using Cronbach's alpha is as follows (table 3.3), however, a greater number of items in the test can artificially increase the value of alpha and a sample with a narrow range can lower it (Manerikar & Manerika, 2015).

Table 3.3: Reliability Levels

| Internal consistency | Cronbach's alpha |
|----------------------|------------------------|
| Very reliable | $\alpha \geq 0.90$ |
| Good | $0.70 = \alpha < 0.90$ |
| Acceptable | $0.60 = \alpha < 0.70$ |
| Poor | $0.50 = \alpha < 0.60$ |
| Unacceptable | $\alpha < 0.50$ |

Furthermore, Factor analysis is a useful tool for investigating variable relationship for complex concepts. Since the sample was greater than 150 to establish dimensionality of constructs and validity of the independent variables, factor analysis is the best option to analyse the dataset (Pallant, 2016; Mwiya et al., 2017).

In every factor analysis, there are the same numbers of factors as there are variables. Each factor captures a certain amount of the overall variance in the observed variables and the factors are always listed in order of how much variation they explain (Jiunn-Woei & Yen, 2014). The factor analysis is an explorative analysis; it groups similar variables into dimension. This process is also called identifying latent variables. Since factor analysis is an explorative analysis it doesn't distinguish between independent and dependent variables (Chan-Kook,

Hyun-Jae & Yang-Soo, 2014). Factor analysis is used in theory testing to verify scale construction and operational.

According to Gajbhiye, Sharma and Awasthi (2015), Principal Component Analysis (PCA) is a powerful tool that attempts to explain the variance of a large dataset of inter-correlated variables with a smaller set of independent variables. The PCA technique extracts the Eigen values and Eigen vectors from the covariance matrix of original variables. Sharma and Mishra (2014) indicate that since PCA is so dependent on the total variance of the original variables, it is most suitable when all the variables are measured in the same units.

According to Karamizadeh, Abdullah, Manaf and Hooman (2013), PCA manages the entire data for analysis without taking into consideration the fundamental class structure and examines the directions that have widest variations. Shlens (2014) affirms that PCA is a standard tool in modern data analysis, in diverse fields from neuroscience to computer graphics, because it is a simple, non-parametric method for extracting relevant information from confusing data sets and PCA provides a road map for how to reduce a complex data set to a lower dimension to reveal the sometimes hidden, simplified structures that often underlie it.

PCA is a bias transformation to diagnosis an estimate of the covariance matrix of the data. See below the PCA equation (Wang, 2014):

$$\bar{y} = \frac{1}{n} \sum_{i=1}^n xi \quad 3.1$$

Before the PCA conducted, sampling adequacy was tested using Kaiser-Meyer-Olkin (KMO), along with data relationship strength using Bartlett's test. The purpose of principal analysis is to reduce a number of observed variables into a relatively smaller number of components and thus identify factors that are significant for the study.

The sampling adequacy was tested using Kaiser-Meyer-Olkin (KMO). According to Hadi, Abdullah and Sentosa (2016), the adequacy of the sample is measured by KMO in SPSS. The sampling is adequate or sufficient if the value of Kaiser Meyer Olkin (KMO) is larger than 0.5; if the KMO is below 0.5 it is unacceptable and factor analysis shouldn't be performed. According to (Hartley & Furr, 2017; Lee, Moy & Hairi, 2017) bare minimum of 0.00 to 0.49 are unacceptable, 0.50 to 0.59 are miserable, 0.60 to 0.69 are mediocre, 0.70 to 0.79 middling,

0.80 to 0.89 meritorious and 0.90 to 1.00 marvellous as recommended by Kaiser in 1974. The formula for the KMO test is:

$$KMO_j = \frac{\sum_{i \neq j} r_{ij}^2}{\sum_{i \neq j} r_{ij}^2 + \sum_{i \neq j} u} \quad 3.2$$

According to Pallant (2016), the Bartlett's Test checks if the observed correlation matrix $R = (r_{ij}) (p \times p)$ diverges significantly from the identity matrix. In order to measure the overall relationship between the technology adoption variables, we computed the determinant of the correlation matrix $|R|$. Under H_0 , $|R|=1$: If the variables are highly correlated, we have $|R| \approx 0$. The Bartlett's Test static indicates to what extent we deviate from the reference situation $|R|=1$. It uses the following formula:

$$x^2 = -\left(n - 1 - \frac{2p+5}{6}\right) \times \ln|R| \quad 3.3$$

In addition, Pearson correlations were conducted to evaluate the proposed framework (see figure 3.4 below) and establish if there is any relationship between the technology adoptions related factors. According to Gogtay and Thatte (2017), Pearson correlation coefficient is a technique for investigating the relationship between two quantitative, continuous variables. Pearson correlation coefficient doesn't attempt to establish if there are dependent and independent variables. Pearson's correlation coefficient (r) is a measure of the strength of the association between the two variables. See formula below to calculate the coefficient:

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]}} \quad 3.4$$

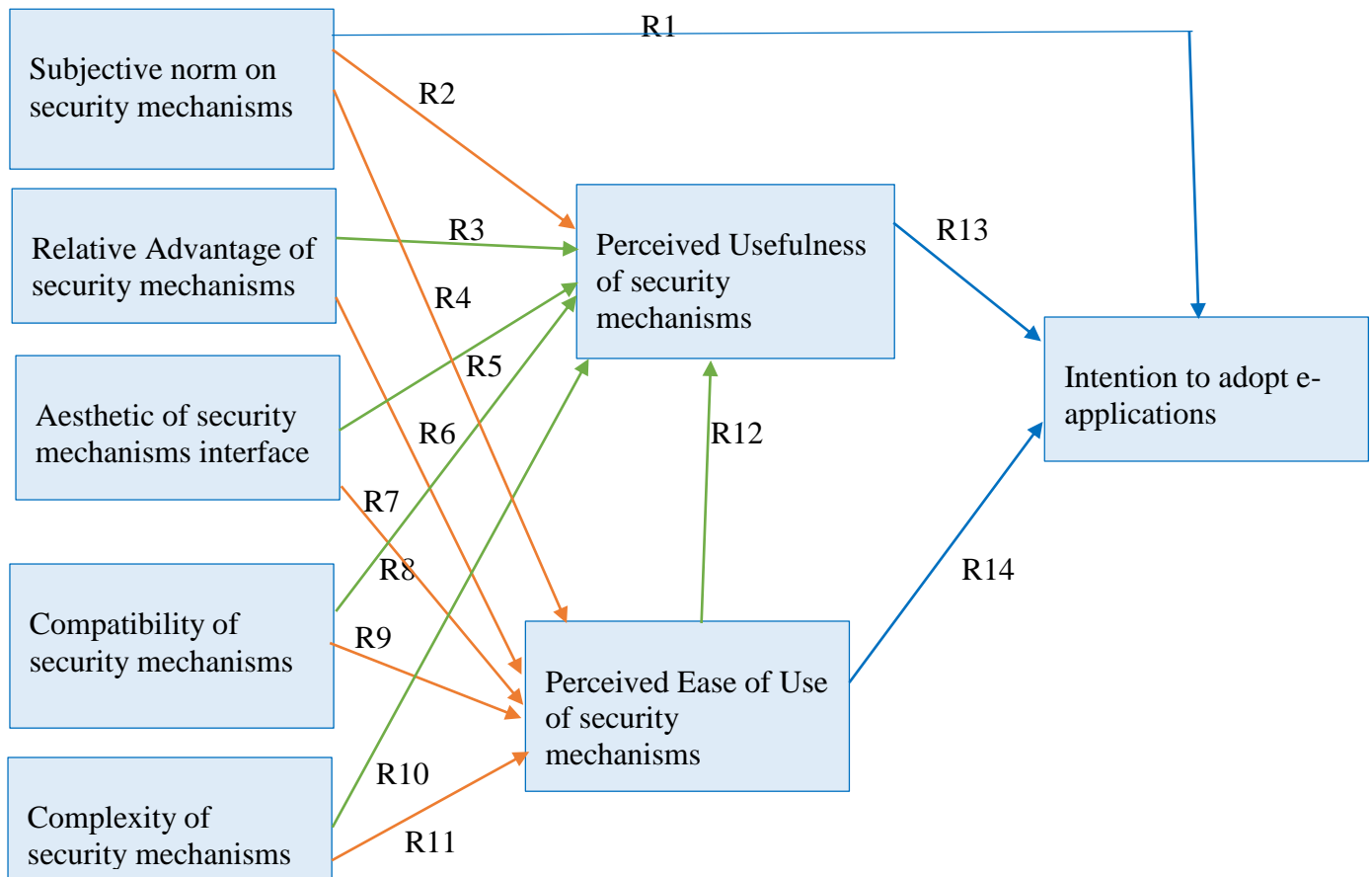


Figure 3.2: Relationships between the users' perceptions on the security of mobile computing for adoption of e-applications

Lastly, for testing the hypotheses in this study multiple linear regression was used between independent variables and dependent variables (see figure 3.3 below). According to Gupta and Dubey (2016), the variable whose value is to be predicted is known as the dependent variable and the ones whose known values are used for prediction are called independent (exploratory) variables. In this study, a dependent variable ITA (Intention to Adopt e-applications) variable is modelled as a function of two independent variables (Perceived Usefulness of security mechanisms and Perceived Ease of Use of security mechanisms).

Furthermore, a dependent variable PU (Perceived Usefulness of security mechanisms) is modelled as a function of six variables (Perceived Ease of Use of security mechanisms, Relative Advantage of security mechanisms, Complexity of security mechanisms, Aesthetics of security mechanisms interface, Compatibility of security mechanisms and Subjective norm on security mechanisms). Furthermore, Perceived Ease of Use of security mechanisms is used as a dependent variable for a few independent variables namely, Relative Advantage of security

mechanisms, Complexity of security mechanisms, Aesthetics of security mechanisms interface, Compatibility of security mechanisms and Subjective norm on security mechanisms.

According to Angelache and Sacla (2016) multiple linear regression is referred to two or more independent variables used to predict the value of a dependent variable. It is also the obvious generalization of simple regression to the situation where we have more than one predictor. Multiple linear regressions are used for modelling the relation between two or more explicative variables and the responses variables by identifying a linear equation between the observed data. For each value of the independent variable x it is associated a value of dependent variable y . Angelache and Sacla (2016) affirm that the individual values of the registered explanatory variables within the linear regression x_1, x_2, \dots, x_p are defined as

$$y = bx + a$$

3.5

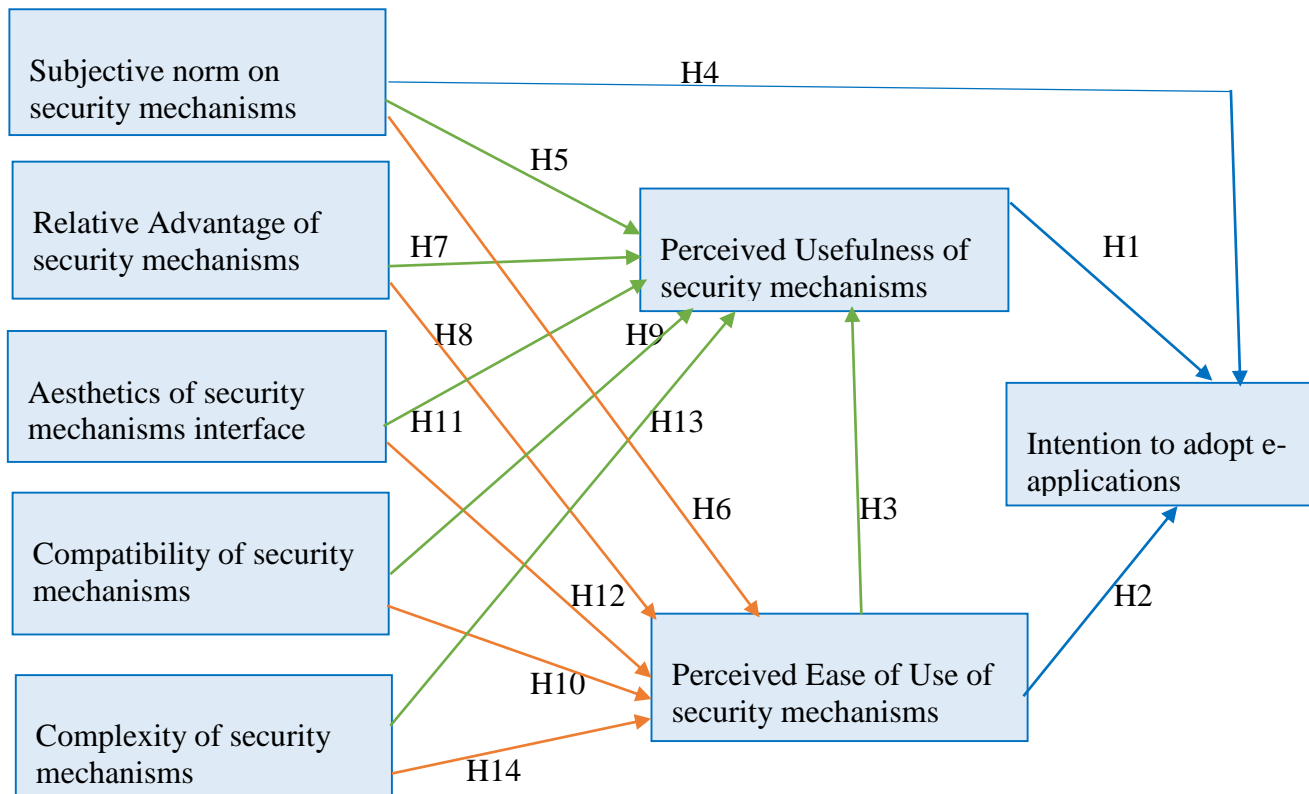


Figure 3.3: Study Hypotheses

After assessing the literature review and the previous studies, the following hypotheses were used:

(i) Perceived Usefulness of Security Mechanisms

The literature review of this study provided evidence of and supports the relevance and the positive significance effect on Perceived Usefulness on users' intention to adopt e-applications.

According to Chin and Lin (2016), **Perceived Usefulness** is defined as the degree to which a person believes that using a system will enhance his or her job performance. The main reason users venture into e-applications is because they find them convenient and useful. Therefore, in this study we tested the following hypothesis:

H1: Perceived Usefulness of security mechanisms has a positive influence on intention to adopt e-applications

(ii) Perceived Ease of Use of Security Mechanisms

A study conducted by Dai (2015) identified that perceived ease of use has a significant effect on attitude. **Perceived Ease of Use** is defined as the degree to which a person believes that using a particular system would be free of effort (Santouridis & Kyritsi, 2014). A complex system of e-applications might act as barrier to users to adopt e-applications. Therefore, Perceived Ease of Use has been identified as a positively predicting factor for users' intention to adopt new technology (Goswami, 2017). In this study it is hypothesized that Perceived Ease of Use of security mechanisms would have a positive effect on users' Perceived Usefulness of security mechanisms and also on Intention to adopt e-applications. Hence, the following hypotheses were tested:

H2: Perceived Ease of Use of security mechanisms has a positive influence on Intention to adopt e-applications.

H3: Perceived Ease of Use of security mechanisms has a positive influence on Perceived Usefulness of security mechanisms.

(iii) Subjective Norm on security mechanisms

Zogheib and Rabaa'i (2015) define **subjective norm** as the degree to which an individual perceives that most people who are important to him or her think he/she should or should not

use the system. Therefore, more pressure will influence the users to adopt e-applications. Hence, in this study we tested the following hypotheses:

H4: Subjective norm on security mechanisms has a positive influence on Intention to adopt e-applications.

H5: Subjective norm on security mechanisms has a positive influence on Perceived Usefulness of security mechanisms.

H6: Subjective norm on security mechanisms has a positive influence on Perceived Ease of Use of security mechanisms.

(iv) Relative Advantage Security Mechanisms

According to Poorangi, Khin, Nikoonejad and Kardevani (2013), **Relative Advantage** refers to the degree to which an innovation is perceived as better than the idea it supersedes by a particular group of users, measured in terms that matter to those users. The greater the Perceived Relative Advantage of an innovation, the more rapid its rate of adoption is likely to be. Thus, in correspondence with the literature review, this study tested the following hypotheses:

H7: Relative Advantage of security mechanisms has a positive influence on Perceived Usefulness security mechanisms.

H8: Relative Advantage of security mechanisms has a positive influence on Perceived Ease of Use of security mechanisms.

(v) Compatibility of Security Mechanisms

Mathur and Verma (2014), define **compatibility** as the degree to which an innovation is perceived as being consistent with the values, experience and needs of the potential adopters. The higher the compatibility of innovation the more the users tend to use it. Hence, in this study we tested the following hypotheses:

H9: Compatibility of security mechanisms has a positive influence on perceived usefulness of security mechanisms.

H10: Compatibility of security mechanisms has a positive influence on perceived ease of use of security mechanisms.

(vi) Aesthetics of security mechanisms interface

Salimun (2013), refers to **aesthetics** as the formal study of art, especially in relation to the idea of beauty. Reinecke et al. (2013) show that Aesthetic is described as the visual appeal. According to Thielsch, Engel & Hirschfeld (2015), most studies found that an aesthetically designed interface is perceived as better quality than a less aesthetical interface; such qualities include perceived ease of use and perceived usefulness. Aesthetics is based on form, colour, tone and texture and aesthetic perceptions appear to have a strong impact on subjective usability evaluation. In this study we tested the following hypotheses:

H11: Aesthetics of security mechanisms interface input interface has a positive influence on Perceived Usefulness of security mechanisms.

H12: Aesthetics of security mechanisms interface has a positive influence on Perceived Ease of Use of security mechanisms.

(vii) Complexity of security mechanisms

Herzallah and Mukhtar (2015) define complexity as the extent to which an innovation can relatively be difficult to understand, learn and use. Complexity of a system or new technology lowers the rate of adoption. Therefore, in this study we tested the following hypotheses:

H13: Complexity of security mechanisms has a negative influence on Perceived Usefulness of security mechanisms.

H14: Complexity of security mechanisms has a negative influence on Perceived Ease of Use of security mechanisms.

(viii) Intention to Adopt e-applications

According to Alsamydai (2014), behaviour intention to use refers to an individual's willingness to perform or not to perform a specific future behaviour. Guritno and Siringoringo (2013) note that behaviour intention to use is influenced by attitude towards using and Perceived Usefulness.

3.11 STUDY LIMITATIONS

The study was conducted in South Africa and only involved users who have access to mobile devices as participants during the process of gathering data. Therefore, the questionnaires were conducted in a common language which is English, with technology terms that had an off-putting outcome for users' understanding. Also the time for data collection was limited to weeks in order to have enough time to analyse data for presentation and interpretation.

3.12 VALIDITY AND RELIABILITY

3.12.1 VALIDITY

Validity refers to the degree that an instrument actually measures what it is designed or intended to measure (Aila & Ombok, 2015). It is also the extent to which an instrument measures what it is supposed to measure and performs as it is designed to perform. In this study the design of the questionnaire was taken from literature and other scholars like Davis and Bagozzi (1989). Therefore, the validity had already been established and assured.

3.12.2 RELIABILITY

Reliability of the questionnaires based on users' perceptions on security of mobile computing was conducted using Cronbach's α efficient proposed by Cronbach in 1951. Cronbach's α efficient is one of the most commonly used measures of reliability in social science studies. Reliability is used to ensure the consistency of the results for the various elements being tested within each factor (Sharma, 2016). It is normally evaluated by assessing the internal consistency of the elements representing each variable using Cronbach's α .

3.13 SUMMARY OF CHAPTER 3

In this chapter the conceptual research model was formulated based on literature pertaining to technology acceptance models. All the factors in the model were extracted from related mobile computing and e-applications literature, which provide the basis to design the questions contained in the questionnaire. The chapter developed the different hypotheses in the proposed model that will be tested in the next chapter (chapter 4). Also, the study approach and method was explained. This is key to helping the researcher to identify the appropriate methods to apply his/ her research in terms of study design, sample technique, sample size, questionnaire design and the related analysis required. The next chapter will focus on the survey outcomes including the sample profile and the security knowledge of both factors of the research model.

CHAPTER 4: DATA PROCESSING AND ANALYSIS

4.1 INTRODUCTION

In this chapter the results of the data analysis are presented. The data were collected using a survey questionnaire and analysed through IBM Statistical Package for the Social Science (SPSS) version 24 for quantitative analysis. The survey was divided in two sections. The first section was the Demographic Information including Gender, Age, Ethnic Group, and Education Level and Occupation Status. The second section was based on the research purpose, which is investigating the users' perceptions on the security of mobile computing for adoption of e-applications, using the 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree) for every item, then processed in response to the research questions posed in chapter 1 of the study.

Four objectives drove the collection of the data and the following data analysis. Those objectives were to develop a base to investigate what have been done in the literature to create an optimal environment to adopt technologies, to propose a framework for users' perceptions on the security of mobile computing for adoption of e-applications, to evaluate the proposed framework and establish if there is any relationship between the technology adoption factors and also to recommend the most suitable user interface based on the users' perceptions on security of mobile computing to adopt e-applications. These objectives were accomplished. The findings presented in this chapter demonstrate the potential for merging theory and practice.

4.2 RESPONSE RATE

Out of the six hundred (600) sample size that was conveniently selected, four hundred and ninety two (492) respondents returned the surveys. Returned survey percentage is calculated as the number of returned surveys divided by sample size multiplied by 100 (Mavletova, 2013). In this study, the response rate was 82%. However, 16 surveys were found to be incomplete; these were therefore removed from the analysis. Accordingly, 476 surveys representing 96.7% of the sample were analysed. According to Rindfuss, Choe, Tsuya, Bumpass and Tamaki (2015), response rates are more important when the study's purpose is to make generalisations

to a larger population, whereas Hardigan, Popovici and Carvajal (2016) state that a response rate of between 30 and 40 percent is average for questionnaires completed electronically. Petrovcic, Petric and Manfreda (2016) agree that if the response rate is less than 30 percent the value and validity of the method and results are in question. Therefore, in this study this target was met with a response rate of 82%.

4.3 RELIABILITY TEST RESULTS

Cronbach's α was used for measuring the internal consistency between all the constructs of the study. Alwan and Al-Zu'bi (2016) in their study approved that the rule of thumb for the reliability test is that 0.70 or higher represents very reliable and consistent. Based on the results in table 4.1, the Cronbach's α for all constructs in this study are very reliable as the values exceed 0.70, which means there is consistent between the study constructs.

Table 4.1: Reliability Statistics for Study Constructs

| Construct | No. of items | Cronbach's α |
|--|---------------------|---------------------------------------|
| Perceived Usefulness of security mechanisms | 4 | 0.764 |
| Perceived Ease of Use of security mechanisms | 4 | 0.828 |
| Intention to Adopt e-applications | 4 | 0.829 |
| Subjective norm on security mechanisms | 3 | 0.850 |
| Relative Advantage of Security Mechanisms | 4 | 0.782 |
| Aesthetics of security mechanisms interface | 4 | 0.783 |
| Compatibility of security mechanisms | 3 | 0.814 |
| Complexity of security mechanisms | 4 | 0.787 |

4.4 VALIDITY TEST RESULTS

For the validity test, factor analysis through Principal Component Analysis (PCA) using varimax rotation was conducted to determine the underlying constructs of the study items (30 items). Prior to this, the sampling adequacy and sphericity were tested by Kaiser-Meyer-Olkin (KMO) and Bartlett's Test of Sphericity respectively to examine the appropriateness of factor analysis. Taking a 95% level of significance $\alpha=0.05$, the p value (sig.) of .000, therefore the factor analysis is valid. As shown in table 4.2, the approximate chi-square is 16492.922 with 435 degrees of freedom that is significant at 0.000 level of significance, with the Kaiser-Meyer-Olkin statistic of 0.904 that is greater than 0.50. Hence factor analysis for users' perceptions on security of mobile computing for adoption of e-applications questionnaire is considered as an appropriate technique for further analysis of the data.

Table 4. 2: Sample Adequate

| | | |
|---|--------------------|-----------|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy | | .904 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 16492.922 |
| | Df | 435 |
| | Sig. | .000 |

Based on table 4.3, on the basis of Varimax Rotation with Kaiser Normalization, 5 factors have been extracted. Each factor is constituted of all those variables that have factor loadings greater than 0.50. Thirty (30) items were clubbed into 5 factors; 5 factors with Eigen values greater than 1 were extracted from the 30 items used in the study; these factors explained for 70.27% of the variability of the users' perceptions on security of mobile computing for adoption of e-applications.

Table 4.3: Eigen Values-Total Variance explained

| Component | Initial Eigen values | | | Rotation Sums of Squared Loadings | | |
|-----------|----------------------|---------------|--------------|-----------------------------------|---------------|--------------|
| | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % |
| 1 | 14.331 | 47.768 | 47.768 | 5.629 | 18.762 | 18.762 |
| 2 | 2.398 | 7.995 | 55.763 | 4.693 | 15.643 | 34.405 |
| 3 | 1.822 | 6.072 | 61.835 | 4.170 | 13.899 | 48.304 |
| 4 | 1.371 | 4.570 | 66.405 | 3.373 | 11.243 | 59.547 |
| 5 | 1.160 | 3.865 | 70.270 | 3.217 | 10.723 | 70.270 |
| 6 | .947 | 3.156 | 73.426 | | | |
| 7 | .838 | 2.794 | 76.220 | | | |
| 8 | .789 | 2.630 | 78.849 | | | |
| 9 | .664 | 2.213 | 81.063 | | | |
| 10 | .651 | 2.170 | 83.233 | | | |
| 11 | .620 | 2.068 | 85.301 | | | |
| 12 | .567 | 1.890 | 87.191 | | | |
| 13 | .524 | 1.746 | 88.937 | | | |
| 14 | .486 | 1.621 | 90.558 | | | |
| 15 | .463 | 1.543 | 92.101 | | | |
| 16 | .372 | 1.239 | 93.339 | | | |
| 17 | .326 | 1.086 | 94.425 | | | |
| 18 | .305 | 1.016 | 95.441 | | | |

| | | | | | | |
|----|------|------|---------|--|--|--|
| 19 | .278 | .928 | 96.369 | | | |
| 20 | .232 | .773 | 97.141 | | | |
| 21 | .221 | .737 | 97.878 | | | |
| 22 | .182 | .607 | 98.485 | | | |
| 23 | .132 | .438 | 98.923 | | | |
| 24 | .115 | .382 | 99.305 | | | |
| 25 | .067 | .223 | 99.529 | | | |
| 26 | .058 | .192 | 99.720 | | | |
| 27 | .048 | .161 | 99.881 | | | |
| 28 | .020 | .066 | 99.947 | | | |
| 29 | .009 | .029 | 99.976 | | | |
| 30 | .007 | .024 | 100.000 | | | |

Extraction Method: Principal Component Analysis.

The matrix gives the correlation of the variables with each of the extracted factors, identified variables included in each factor; the variable with the value maximum in each row is selected to be part of the respective factor. The values are highlighted in each of the rows to group the 30 items into 8 core factors. As can be seen in table 4.4, the factor loadings greater than 0.50 are highlighted; these factors can confirm that the items are measured; just one construct is satisfied and valid.

Table 4.4: Factor Loadings

| Rotated Component Matrix | | | | | | | | |
|--------------------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| | PU | PEOU | AEST | RAD | SN | COMPL | COM | ITA |
| PU1 | .255 | .633 | .251 | .070 | .365 | .134 | .207 | .100 |
| PU2 | .217 | .751 | .195 | .109 | .191 | .007 | -.063 | .180 |
| PU3 | .075 | .232 | .114 | .131 | .678 | .143 | .418 | -.029 |
| PU4 | .193 | .404 | .146 | .091 | .238 | .286 | .509 | -.018 |
| PEOU1 | .190 | .119 | .629 | .260 | .261 | .125 | .128 | .150 |
| PEOU2 | .127 | .275 | .782 | .080 | .013 | .247 | .181 | -.017 |
| PEOU3 | .092 | .202 | .764 | .187 | .047 | .179 | .154 | .007 |
| PEOU4 | .128 | .120 | .649 | .140 | .377 | .033 | .098 | .216 |
| AEST1 | .279 | .251 | .391 | .246 | .514 | .010 | .261 | .197 |
| AEST2 | .071 | .242 | .116 | .113 | .868 | .180 | .102 | -.003 |
| AEST3 | .304 | .681 | .087 | -.021 | .097 | .227 | .205 | .357 |
| AEST4 | .290 | .812 | .104 | .213 | .240 | .077 | .095 | .077 |
| RAD1 | .249 | .665 | .136 | .252 | .250 | .211 | .202 | .045 |
| RAD2 | .194 | .644 | .244 | .282 | .145 | .151 | .231 | -.005 |
| RAD3 | .286 | .501 | .364 | .285 | .093 | .257 | .175 | -.157 |
| RAD4 | .088 | .164 | .152 | .217 | -.027 | .241 | .184 | .758 |
| SN1 | .184 | .108 | .244 | .339 | .285 | .406 | .547 | .303 |
| SN2 | .237 | .119 | .247 | .205 | .185 | .821 | .189 | .168 |
| SN3 | .204 | .316 | .232 | .743 | .157 | .281 | .231 | .068 |
| COMPL1 | .894 | .258 | .119 | .148 | .104 | .163 | .128 | .088 |
| COMPL2 | .186 | .315 | .100 | .216 | .225 | .580 | .246 | .038 |

| | | | | | | | | |
|--------|------|------|------|------|-------|------|------|-------|
| COMPL3 | .225 | .138 | .245 | .198 | .193 | .820 | .195 | .177 |
| COMPL4 | .105 | .304 | .154 | .105 | .837 | .225 | .118 | -.022 |
| COM1 | .245 | .378 | .281 | .388 | -.011 | .047 | .648 | -.194 |
| COM2 | .914 | .212 | .125 | .127 | .063 | .133 | .132 | .031 |
| COM3 | .909 | .205 | .117 | .136 | .078 | .119 | .106 | .005 |
| ITA1 | .229 | .165 | .249 | .205 | .184 | .271 | .761 | .210 |
| ITA2 | .211 | .124 | .220 | .223 | .199 | .234 | .770 | .210 |
| ITA3 | .913 | .162 | .114 | .142 | .093 | .096 | .123 | .043 |
| ITA4 | .219 | .185 | .223 | .854 | .157 | .166 | .149 | .134 |

Extraction Method: Principal Component Analysis

Rotation Method: Varimax with Kaiser Normalization

4.5 QUANTITATIVE ANALYSIS

In order to achieve the observed objectives of the study, the results were analysed and presented as they appear in the different sections of the questionnaire (refer to Appendix B). According to Simpson (2015) a useful first step in the analysis of quantitative data is to examine the frequency distribution for each variable to establish the numerical value that represents the total number of responses for a variable under study. Frequency distribution was undertaken throughout the analysis of the questionnaire findings.

4.5.1 SECTION A: PARTICIPANTS' DEMOGRAPHIC INFORMATION

In order to elaborate on the participants' background, section A of the questionnaire (question 1 to 5) captured the demographic information of the participants including gender, age, ethnic group, educational level and occupational status. The results, which are descriptive in nature, are indicated by means of a frequency table. The analysis was carried out based on the 476 completed surveys that were properly filled out by the South African residents. All of the respondents were participants who have access to mobile devices. Although demographic information is not part of the purpose of the study, this set of data is intended to describe demographic variables of the sample. In terms of gender, 313 (65.8%) are female and 163

(34.2%) are male. In relation to age, 156 (32.8%) of the respondents are 18-25 years old, 230 (48.3%) are 26-35 years old, 71 (14.9%) are 36-45 years old and 19 (4.0%) are over 46 years old. It can be said that the higher percentages are associated with the ages of younger people. In this respect, the relationship between the age of people and e-application adoption is found to support the studies done by (Ameme, 2015, Alwan & Al-Zu'bi, 2016). Elderly participants are less likely to be adopters of e-applications than young people.

In terms of ethnic groups, 396 (83.2%) of the respondents are black, 16 (3.4%) are white, 18 (3.8%) of the respondents are Indian, 35(7.4%) of the respondents are coloured and 11 (2.3%) of the respondents are Asian. It can be concluded that the higher percentages are associated with black people who are dominant at the location where the study is being conducted (South Africa) for adoption of e-applications.

In terms of educational level, 210 (44.1%) of the respondents have degrees, 138 (29.0%) have diplomas, 96 (20.2%) of the respondents had high school certificates, and 32 (6.7%) had other levels of education. It can be concluded that a high education level influences individuals to adopt e-applications. In this case, an association between educational level and user adoption of e-application is found.

In terms of occupation status, 58 (12.2%) of the respondents are not working, 364 (76.4%) of the respondents are working, 6 (1.3%) of the respondents are pensioners, 30 (6.3%) of the respondents are self-employed and 18 (3.8%) of the respondents have other occupation status. It can be said that the higher percentages are associated with the participants who are working. See table 4.5 on the next page:

Table 4.5: Users' Demographic Information

| Category | Item | Frequency | Percentage (%) |
|-------------------|---------------|-----------|----------------|
| Gender | Male | 163 | 34.2 |
| | Female | 313 | 65.8 |
| Age group | 18-25 | 156 | 32.8 |
| | 26-35 | 230 | 48.3 |
| | 36-45 | 71 | 14.9 |
| | Over 46 | 19 | 4.0 |
| Ethnic group | Black | 396 | 83.2 |
| | White | 16 | 3.4 |
| | Indian | 18 | 3.8 |
| | Coloured | 35 | 7.4 |
| | Asian | 11 | 2.3 |
| Education level | High school | 96 | 20.2 |
| | Degree | 210 | 44.1 |
| | Diploma | 138 | 29.0 |
| | Other | 32 | 6.7 |
| Occupation status | Not Working | 58 | 12.2 |
| | Working | 364 | 76.4 |
| | Pensioner | 6 | 1.3 |
| | Self-employed | 30 | 6.3 |
| | Other | 18 | 3.8 |

4.5.2 SECTION B: USERS' PERCEPTIONS OF THE SECURITY OF MOBILE COMPUTING FOR ADOPTION OF E-APPLICATIONS

The questions in section B of the questionnaire (refer to Appendix B) aim to determine:

- How South African residents perceive the security mechanisms for adoption of e-applications
- If South African residents' opinion towards security mechanisms of mobile computing for adoption of e-applications will assist in the recommendation of security mechanisms interface for e-application
- How will South African residents' opinion towards security mechanisms of mobile mechanisms assist with establishing the relationships between the technology factors

In this section, the quantitative analysis employs a format of frequency tables indicating the actual perspectives of respondents. This was followed by an interpretation of the results. The items within section B were checked for reliability and validity (see table 4.2 to table 4.4).

(i) Intention to adopt e-applications

(a) I intend to use the e-applications frequently in my life.

As depicted in table 4.6, 21 (4.4%) of the respondents strongly disagree that they intend to use the e-applications frequently in my life, 63 (13.2%) of the respondents disagree that they intend to use the e-applications frequently in my life, 105 (22.1%) of the respondents neither agree nor disagree that they intend to use the e-applications frequently in my life, 212 (44.5%) of the respondents agree that they intend to use the e-applications frequently in my life and 75 (15.8%) of the respondents strongly agree that they intend to use the e-applications frequently in my life.

Table 4.6: I intend to use the e-applications frequently in my life

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 21 | 4.4 | 4.4 | 4.4 |
| | Disagree | 63 | 13.2 | 13.2 | 17.6 |
| | Neither agree nor disagree | 105 | 22.1 | 22.1 | 39.7 |
| | Agree | 212 | 44.5 | 44.5 | 84.2 |
| | Strongly Agree | 75 | 15.8 | 15.8 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(b) I intend to use e-applications platform as soon as possible.

21 (4.4%) of the respondents strongly disagree that they intend to use e-applications platform as soon as possible, 69 (14.5%) of the respondents strongly disagree that they intend to use e-applications platform as soon as possible, 104 (21.8%) of the respondents neither agree nor disagree that they intend to use e-applications platform as soon as possible, 210 (44.1%) of the respondents agree that they intend to use e-applications platform as soon as possible and 72 (15.1%) of the respondents strongly agree that they intend to use e-applications platform as soon as possible. See table 4.7 below

Table 4.7: I intend to use e-applications platform as soon as possible

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 21 | 4.4 | 4.4 | 4.4 |
| | Disagree | 69 | 14.5 | 14.5 | 18.9 |
| | Neither agree nor disagree | 104 | 21.8 | 21.8 | 40.8 |
| | Agree | 210 | 44.1 | 44.1 | 84.9 |
| | Strongly Agree | 72 | 15.1 | 15.1 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(c) I plan to use the e-applications platform in the future.

Table 4.8 below shows that 54 (11.3%) of the respondents strongly disagree that they plan to use the e-applications platform in the future, 92 (19.3%) of the respondents disagree that they plan to use the e-applications platform in the future, 177 (37.2%) of the respondents neither agree nor disagree that they plan to use the e-applications platform in the future, 108 (22.7%) of the respondents agree that they plan to use the e-applications platform in the future and 45

(9.5%) of the respondents strongly agree that they plan to use the e-applications platform in the future.

Table 4.8: I plan to use the e-applications platform in the future

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 54 | 11.3 | 11.3 | 11.3 |
| | Disagree | 92 | 19.3 | 19.3 | 30.7 |
| | Neither agree nor disagree | 177 | 37.2 | 37.2 | 67.9 |
| | Agree | 108 | 22.7 | 22.7 | 90.5 |
| | Strongly Agree | 45 | 9.5 | 9.5 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(d) I will recommend e-applications to others.

The results of the survey suggested that most of the respondents 180 (37.8%) agree that they will recommend e-applications to others. However, 120 (25.2%) of the respondents neither agree nor disagree that they will recommend e-applications to others, further 79 (16.6%) of the respondents strongly agree that they will recommend e-applications to others. 79 (16.6%) of the respondents disagree that they will recommend e-applications to others, 18 (3.8%) of the respondents strongly disagree that they will recommend e-applications to others. See table 4.9 below:

Table 4.9: I will recommend e-applications to others

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 18 | 3.8 | 3.8 | 3.8 |
| | Disagree | 79 | 16.6 | 16.6 | 20.4 |
| | Neither agree nor disagree | 120 | 25.2 | 25.2 | 45.6 |
| | Agree | 180 | 37.8 | 37.8 | 83.4 |
| | Strongly Agree | 79 | 16.6 | 16.6 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(ii) Perceived Usefulness of security mechanisms

(a) I find using Password/PIN security mechanism on mobile computing useful to access e-applications

Respondents were asked to select the level of agreement with the Perceived Usefulness of Security Mechanisms statement appropriate to them (see table 11 below); all the respondents answered the question (476 responses). The largest group accounted for 180 (37.8%) Agree that they find using Password/PIN security mechanism on mobile computing useful to access e-applications, followed by 136 (28.6%) of respondents who neither agree nor disagree that they find using Password/PIN security mechanism on mobile computing useful to access e-applications, 68 (14.3%) of the respondents strongly agree that they find using Password/PIN security mechanism on mobile computing useful to access e-applications, 64 (13.4%) of the respondents disagree that they find using Password/PIN security mechanism on mobile computing useful to access e-applications, and lastly, 28 (5.9%) of respondents strongly disagree that they find using Password/PIN security mechanism on mobile computing useful to access e-applications. See table 4.10 below:

Table 4.10: Password/PIN security mechanism perceived usefulness

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 28 | 5.9 | 5.9 | 5.9 |
| | Disagree | 64 | 13.4 | 13.4 | 19.3 |
| | Neither agree nor disagree | 136 | 28.6 | 28.6 | 47.9 |
| | Agree | 180 | 37.8 | 37.8 | 85.7 |
| | Strongly Agree | 68 | 14.3 | 14.3 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(b) I find using fingerprint security mechanism on mobile computing useful to access e-applications

In table 4.11 below, out of 476 respondents, 127 (26.7%) agree that they find using fingerprint on mobile computing useful to access e-applications, 103 (21.6%) of the respondents disagree that they find using fingerprint security mechanism on mobile computing useful to access e-applications, 63 (13.2%) of the respondents strongly agree that they find using fingerprint security mechanism on mobile computing useful to access e-applications, 54 (11.3%) of the

respondents strongly disagree that they find using fingerprint security mechanism on mobile computing useful to access e-applications and 129(27.1%) of the respondents neither agree nor disagree that they find using fingerprint security mechanism on mobile computing useful to access e-applications.

Table 4.11: Finger print security mechanism perceived usefulness

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 54 | 11.3 | 11.3 | 11.3 |
| | Disagree | 103 | 21.6 | 21.6 | 33.0 |
| | Neither agree nor disagree | 129 | 27.1 | 27.1 | 60.1 |
| | Agree | 127 | 26.7 | 26.7 | 86.8 |
| | Strongly Agree | 63 | 13.2 | 13.2 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(c) I find using combination of password and fingerprint security mechanism on mobile computing useful to access e-applications

As depicted in table 4.12 below, 162 (34.0%) of the respondents agree that they find using combination of password and fingerprint on mobile computing useful to access e-applications, 59 (12.4%) of the respondents strongly agree that they find using combination of password and fingerprint security mechanism on mobile computing useful to access e-applications, 155 (32.6%) of the respondents neither agree nor disagree that they find using combination of password and fingerprint security mechanism on mobile computing useful to access e-applications, 74 (15.5%) of the respondents disagree that they find using combination of password and fingerprint security mechanism on mobile computing useful to access e-applications and 26 (5.5%) of the respondents strongly disagree that they find using combination of password and fingerprint security mechanism on mobile computing useful to access e-applications.

Table 4.12: Combination of password and fingerprint security mechanism perceived usefulness

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly agree | 26 | 5.5 | 5.5 | 5.5 |
| | Disagree | 74 | 15.5 | 15.5 | 21.0 |
| | Neither agree nor disagree | 155 | 32.6 | 32.6 | 53.6 |
| | Agree | 162 | 34.0 | 34.0 | 87.6 |
| | Strongly agree | 59 | 12.4 | 12.4 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(d) I find using pattern security mechanism on mobile computing useful to access e-applications

169 (35.5%) of the respondents agree that they find using pattern security mechanism on mobile computing useful to access e-applications, 139 (29.2%) of the respondents neither agree nor disagree that they find using pattern security mechanism on mobile computing useful to access e-applications, 58 (12.2%) of the respondents strongly agree that they find using pattern security mechanism on mobile computing useful to access e-applications, 79 (16.6%) of the respondents disagree that they find using pattern security mechanism on mobile computing useful to access e-applications. Lastly, 31 (6.5%) of the respondents strongly disagree that they find using pattern security mechanism on mobile computing useful to access e-applications. See table 4.13 below:

Table 4.13: I find using pattern on mobile computing useful to access e-applications

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly disagree | 31 | 6.5 | 6.5 | 6.5 |
| | Disagree | 79 | 16.6 | 16.6 | 23.1 |
| | Neither agree nor disagree | 139 | 29.2 | 29.2 | 52.3 |
| | Agree | 169 | 35.5 | 35.5 | 87.8 |
| | Strongly Agree | 58 | 12.2 | 12.2 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(iii) Perceived Ease of Use of security mechanisms

(a) I find Password/PIN security mechanism easy to use on mobile computing to access e-applications

126 (26.5%) of the respondents strongly agree that they find Password/PIN security mechanism easy to use on mobile computing to access e-applications, 180 (37.8%) of the respondents agree that they find Password/PIN security mechanism easy to use on mobile computing to access e-applications, 116 (24.4%) of the respondents neither agree nor disagree that they find Password/PIN security mechanism easy to use on mobile computing to access e-applications, 38 (8.0%) of the respondents disagree that they find Password/PIN security mechanism easy to use on mobile computing to access e-applications and 16 (3.4%) of the respondents strongly disagree that they find Password/PIN security mechanism easy to use on mobile computing to access e-applications, see table 4.14 below:

Table 4.14: I find Password/PIN security mechanism easy to use on mobile computing to access e-applications

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 16 | 3.4 | 3.4 | 3.4 |
| | Disagree | 38 | 8.0 | 8.0 | 11.3 |
| | Neither agree nor disagree | 116 | 24.4 | 24.4 | 35.7 |
| | Agree | 180 | 37.8 | 37.8 | 73.5 |
| | Strongly Agree | 126 | 26.5 | 26.5 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(b) I find fingerprint security mechanism easy to use on mobile computing to access e-applications

100 (21.0%) of the respondents strongly agree that they find fingerprint security mechanism easy to use on mobile computing to access e-applications, 171 (35.9%) of the respondents agree that they find fingerprint security mechanism easy to use on mobile computing to access e-applications, 123 (25.8%) of the respondents neither agree nor disagree that they find fingerprint security mechanism easy to use on mobile computing to access e-applications, 66 (13.9%) of the respondents disagree that they find fingerprint security mechanism easy to use

on mobile computing to access e-applications and 16 (3.4%) of the respondents strongly disagree that they find fingerprint security mechanism easy to use on mobile computing to access e-applications. See table 4.15 below:

Table 4.15: I find fingerprint security mechanism easy to use on mobile computing to access e-applications

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 16 | 3.4 | 3.4 | 3.4 |
| | Disagree | 66 | 13.9 | 13.9 | 17.2 |
| | Neither agree nor disagree | 123 | 25.8 | 25.8 | 43.1 |
| | Agree | 171 | 35.9 | 35.9 | 79.0 |
| | Strongly Agree | 100 | 21.0 | 21.0 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(c) I find using combination of password and fingerprint security mechanism easy to use on mobile computing to access e-applications

90 (18.9%) of the respondents strongly agree that they find using combination of password security mechanism and fingerprint easy to use on mobile computing to access e-applications, 177 (37.2%) of the respondents agree that they find using combination of password and fingerprint security mechanism easy to use on mobile computing to access e-applications, 138 (29.0%) of the respondents neither agree nor disagree that they find using combination of password and fingerprint security mechanism easy to use on mobile computing to access e-applications, 56 (11.8%) of the respondents disagree that they find using combination of password and fingerprint security mechanism easy to use on mobile computing to access e-applications and 15 (3.2%) of the respondents strongly disagree that they find using combination of password and fingerprint security mechanism easy to use on mobile computing to access e-applications, as illustrated on table 4.16.

Table 4. 16: I find using combination of password and fingerprint security mechanism easy to use on mobile computing to access e-applications

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 15 | 3.2 | 3.2 | 3.2 |
| | Disagree | 56 | 11.8 | 11.8 | 14.9 |
| | Neither agree nor disagree | 138 | 29.0 | 29.0 | 43.9 |
| | Agree | 177 | 37.2 | 37.2 | 81.1 |
| | Strongly Agree | 90 | 18.9 | 18.9 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(d) I find using pattern security mechanism on mobile computing easy to use to access e-applications

In table 4.17 below, 165 (34.7%) of the respondents agree that they find using pattern security mechanism on mobile computing easy to use to access e-applications, 90 (18.9%) of the respondents strongly agree that they find using pattern security mechanism on mobile computing easy to use to access e-applications, 121 (25.4%) of the respondents neither agree nor disagree that they find using pattern security mechanism on mobile computing easy to use to access e-applications, 55 (11.6%) of the respondents disagree that they find using pattern security mechanism on mobile computing easy to use to access e-applications and 45 (9.5%) of the respondents strongly disagree that they find using pattern security mechanism on mobile computing easy to use to access e-applications.

Table 4.17: I find using pattern security mechanism on mobile computing easy to use to access e-applications

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 45 | 9.5 | 9.5 | 9.5 |
| | Disagree | 55 | 11.6 | 11.6 | 21.0 |
| | Neither agree nor disagree | 121 | 25.4 | 25.4 | 46.4 |
| | Agree | 165 | 34.7 | 34.7 | 81.1 |
| | Strongly Agree | 90 | 18.9 | 18.9 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(iv) Aesthetics of security mechanisms interface

(a) Security mechanisms' interface is clearly structured and simple

85 (17.9%) of the respondents strongly agree that the security mechanisms' interface is clearly structured and simple, 186 (39.1%) of the respondents agree that the security mechanisms' interface is clearly structured and simple, 132 (27.7%) of the respondents neither agree nor disagree that that the security mechanisms' interface is clearly structured and simple, 46 (9.6%) of the respondents disagree that the security mechanisms' interface is clearly structured and simple and 27 (5.7%) of the respondents strongly disagree that the security mechanisms' interface is clearly structured and simple; see table 4.18 below:

Table 4.18: Security mechanisms' interface is clearly structured and simple

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 27 | 5.7 | 5.7 | 5.7 |
| | Disagree | 46 | 9.7 | 9.7 | 15.3 |
| | Neither agree nor disagree | 132 | 27.7 | 27.7 | 43.1 |
| | Agree | 186 | 39.1 | 39.1 | 82.1 |
| | Strongly Agree | 85 | 17.9 | 17.9 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(b) Security mechanisms' interface is beautiful

As depicted in table 4.19 below, 158 (33.2%) of the respondents agree that security mechanisms' interface is beautiful, 72 (15.1%) of the respondents strongly agree that security mechanisms' interface is beautiful, 137 (28.8%) of the respondents neither agree nor disagree that security mechanisms' interface is beautiful, 67 (14.1%) of the respondents disagree that security mechanisms' interface is beautiful and 42 (8.8%) of the respondents strongly disagree that security mechanisms' interface is beautiful.

Table 4.19: Security mechanisms' interface is beautiful

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 42 | 8.8 | 8.8 | 8.8 |
| | Disagree | 67 | 14.1 | 14.1 | 22.9 |
| | Neither agree nor disagree | 137 | 28.8 | 28.8 | 51.7 |
| | Agree | 158 | 33.2 | 33.2 | 84.9 |
| | Strongly Agree | 72 | 15.1 | 15.1 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(c) The user interface for security mechanisms' input is designed for all levels of users.

116 (24.4%) of the respondents agree that the user interface for security mechanisms' input is designed for all levels of users, 133 (27.9%) of the respondents neither agree nor disagree that the user interface for security mechanisms' input is designed for all levels of users, 38 (8.0%) of the respondents strongly agree that the user interface for security mechanisms' input is designed for all levels of users, 142 (29.8%) of the respondents disagree that the user interface for security mechanisms' input is designed for all levels of users. Lastly, 47 (9.9%) of the respondents strongly disagree that the user interface for security mechanisms' input is designed for all levels of users. See table 4.20 below:

Table 4.20: The user interface for security mechanisms' input is designed for all levels of users.

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 47 | 9.9 | 9.9 | 9.9 |
| | Disagree | 142 | 29.8 | 29.8 | 39.7 |
| | Neither agree nor disagree | 133 | 27.9 | 27.9 | 67.6 |
| | Agree | 116 | 24.4 | 24.4 | 92.0 |
| | Strongly Agree | 38 | 8.0 | 8.0 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(d) Security mechanisms' interface is stylish

In table 4.21 below, out of 476 respondents, 156 (32.8%) agree that security mechanisms' interface is stylish, 86 (18.1%) of the respondents disagree that security mechanisms' interface

is stylish, 80 (16.8%) of the respondents strongly agree that security mechanisms' interface is stylish, 50 (10.5%) of the respondents strongly disagree that security mechanisms' interface is stylish and 104 (21.8%) of the respondents neither agree nor disagree that security mechanisms' interface is stylish.

Table 4.21: Security mechanisms' interface is stylish

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 50 | 10.5 | 10.5 | 10.5 |
| | Disagree | 86 | 18.1 | 18.1 | 28.6 |
| | Neither agree nor disagree | 104 | 21.8 | 21.8 | 50.4 |
| | Agree | 156 | 32.8 | 32.8 | 83.2 |
| | Strongly Agree | 80 | 16.8 | 16.8 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(v) Relative Advantage of security mechanisms

(a) PIN/Password security mechanism has more advantages that makes the security more efficient.

In table 4.22 below, 172 (36.1%) of the respondents agree that PIN/Password security mechanism has more advantages that make the security more efficient, 79 (16.6%) of the respondents strongly agree that PIN/Password security mechanism has more advantages that make the security more efficient, 123 (25.8%) of the respondents neither agree nor disagree that PIN/Password security mechanism has more advantages that make the security more efficient, 70 (14.7%) of the respondents disagree that PIN/Password security mechanism has more advantages that make the security more efficient and 32 (6.7%) of the respondents strongly disagree that PIN/Password security mechanism has more advantages that make the security more efficient.

Table 4.22: PIN/Password security mechanism has more advantages that make the security more efficient

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 32 | 6.7 | 6.7 | 6.7 |
| | Disagree | 70 | 14.7 | 14.7 | 21.4 |
| | Neither agree nor disagree | 123 | 25.8 | 25.8 | 47.3 |
| | Agree | 172 | 36.1 | 36.1 | 83.4 |
| | Strongly Agree | 79 | 16.6 | 16.6 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(b) Fingerprint security mechanism has more advantages that make the security more efficient.

85 (17.9%) of the respondents strongly agree that fingerprint security mechanism has more advantages that make the security more efficient, 165 (34.7%) of the respondents agree that fingerprint security mechanism has more advantages that make the security more efficient, 109 (22.9%) of the respondents neither agree nor disagree that fingerprint security mechanism has more advantages that make the security more efficient, 87 (18.3%) of the respondents disagree that fingerprint security mechanism has more advantages that make the security more efficient and 30 (6.3%) of the respondents strongly disagree that fingerprint security mechanism has more advantages that make the security more efficient; see table 4.23 below:

Table 4.23: fingerprint security mechanism has more advantages that make the security more efficient

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 30 | 6.3 | 6.3 | 6.3 |
| | Disagree | 87 | 18.3 | 18.3 | 24.6 |
| | Neither agree nor disagree | 109 | 22.9 | 22.9 | 47.5 |
| | Agree | 165 | 34.7 | 34.7 | 82.1 |
| | Strongly Agree | 85 | 17.9 | 17.9 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(c) Pattern security mechanism has more advantages that make the security more efficient.

66 (13.9%) of the respondents strongly agree that pattern security mechanism has more advantages that make the security more efficient, 181 (38.0%) of the respondents agree that pattern security mechanism has more advantages that make the security more efficient, 134 (28.2%) of the respondents neither agree nor disagree that pattern security mechanism has more advantages that make the security more efficient, 76 (16.0%) of the respondents disagree that pattern security mechanism has more advantages that make the security more efficient and 19 (4.0%) of the respondents strongly disagree that pattern security mechanism has more advantages that make the security more efficient; see table 4.24 below:

Table 4.24: Pattern security mechanism has more advantages which makes the security more efficient

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 19 | 4.0 | 4.0 | 4.0 |
| | Disagree | 76 | 16.0 | 16.0 | 20.0 |
| | Neither agree nor disagree | 134 | 28.2 | 28.2 | 48.1 |
| | Agree | 181 | 38.0 | 38.0 | 86.1 |
| | Strongly Agree | 66 | 13.9 | 13.9 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(d) Combination of PIN and Fingerprint security mechanism has more advantages that make the security more efficient.

50 (10.5%) of the respondents strongly agree that combination of PIN and Fingerprint security mechanism has more advantages that make the security more efficient, 126 (26.5%) of the respondents agree that combination of PIN and Fingerprint security mechanism has more advantages that make the security more efficient, 140 (29.4%) of the respondents neither agree nor disagree that combination of PIN and Fingerprint security mechanism has more advantages that make the security more efficient, 113 (23.7%) of the respondents disagree that combination of PIN and Fingerprint security mechanism has more advantages that make the security more efficient and 47 (9.9%) of the respondents strongly disagree that combination of PIN and Fingerprint security mechanism has more advantages that make the security more efficient; see table 4.25 below:

Table 4.25: Combination of PIN and Fingerprint security mechanism has more advantages that make the security more efficient

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 47 | 9.9 | 9.9 | 9.9 |
| | Disagree | 113 | 23.7 | 23.7 | 33.6 |
| | Neither agree nor disagree | 140 | 29.4 | 29.4 | 63.0 |
| | Agree | 126 | 26.5 | 26.5 | 89.5 |
| | Strongly Agree | 50 | 10.5 | 10.5 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(vi) Subjective norm on security mechanisms

(a) Individuals who influence me think that I should use Password/PIN security mechanism on mobile computing to access e-applications.

As depicted in table 4.26 below, 180 (37.8%) of the respondents agree that individuals who influence me think that I should use Password/PIN security mechanism on mobile computing to access e-applications, 96 (20.2%) of the respondents strongly agree that individuals who influence me think that I should use Password/PIN security mechanism on mobile computing to access e-applications, 117 (24.6%) of the respondents neither agree nor disagree that individuals who influence me think that I should use Password/PIN security mechanism on mobile computing to access e-applications, 63 (13.2%) of the respondents disagree that individuals who influence me think that I should use Password/PIN security mechanism on mobile computing to access e-applications and 20 (4.2%) of the respondents strongly disagree that individuals who influence me think that I should use password/PIN security mechanism on mobile computing to access e-applications.

Table 4.26: Individuals who influence me think that I should use Password/PIN security mechanism on mobile computing to access e-applications

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 20 | 4.2 | 4.2 | 4.2 |
| | Disagree | 63 | 13.2 | 13.2 | 17.4 |
| | Neither agree nor disagree | 117 | 24.6 | 24.6 | 42.0 |
| | Agree | 180 | 37.8 | 37.8 | 79.8 |
| | Strongly Agree | 96 | 20.2 | 20.2 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(b) Individuals who influence me think that I should use fingerprint security mechanism on mobile computing to access e-applications.

85 (17.9%) of the respondents strongly agree that individuals who influence me think that I should use fingerprint security mechanism on mobile computing to access e-applications, 186 (39.1%) of the respondents agree that individuals who influence me think that I should use fingerprint security mechanism on mobile computing to access e-applications, 99 (20.8%) of the respondents neither agree nor disagree that individuals who influence me think that I should use fingerprint security mechanism on mobile computing to access e-applications, 77 (16.2%) of the respondents disagree that individuals who influence me think that I should use fingerprint security mechanism on mobile computing to access e-applications and 29 (6.1%) of the respondents strongly disagree that individuals who influence me think that I should use fingerprint security mechanism on mobile computing to access e-applications; see table 4.27 below:

Table 4.27: Individuals who influence me think that I should use fingerprint security mechanism on mobile computing to access e-applications

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 29 | 6.1 | 6.1 | 6.1 |
| | Disagree | 77 | 16.2 | 16.2 | 22.3 |
| | Neither agree nor disagree | 99 | 20.8 | 20.8 | 43.1 |
| | Agree | 186 | 39.1 | 39.1 | 82.1 |
| | Strongly Agree | 85 | 17.9 | 17.9 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(c) Individuals who influence me think that I should use pattern security mechanism on mobile computing to access e-applications.

91 (19.1%) of the respondents strongly agree that individuals who influence me think that I should use pattern security mechanism on mobile computing to access e-applications, 191 (40.1%) of the respondents agree that individuals who influence me think that I should use pattern security mechanism on mobile computing to access e-applications, 108 (22.7%) of the respondents neither agree nor disagree that individuals who influence me think that I should use pattern security mechanism on mobile computing to access e-applications, 68 (14.3%) of the respondents disagree that individuals who influence me think that I should use pattern security mechanism on mobile computing to access e-applications and 18 (3.8%) of the respondents strongly disagree that individuals who influence me think that I should use pattern security mechanism on mobile computing to access e-applications; see table 4.28 below:

Table 4.28: Individuals who influence me think that I should use pattern security mechanism on mobile computing to access e-applications

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 18 | 3.8 | 3.8 | 3.8 |
| | Disagree | 68 | 14.3 | 14.3 | 18.1 |
| | Neither agree nor disagree | 108 | 22.7 | 22.7 | 40.8 |
| | Agree | 191 | 40.1 | 40.1 | 80.9 |
| | Strongly Agree | 91 | 19.1 | 19.1 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(vii) Compatibility of security mechanisms

(a) The function of PIN/Password security mechanism is compatible for e-applications on mobile device.

In table 4.29 below, 167 (35.1%) of the respondents agree that the function of PIN/Password is compatible for e-applications on mobile device, 85 (17.9%) of the respondents strongly agree that the function of PIN/Password is compatible for e-applications on mobile device, 91 (19.1%) of the respondents neither agree nor disagree that the function of PIN/Password is

compatible for e-applications on mobile device, 87 (18.3%) of the respondents disagree that the function of PIN/Password is compatible for e-applications on mobile device and 46 (9.7%) of the respondents strongly disagree that the function of PIN/Password is compatible for e-applications on mobile device.

Table 4.29: The function of PIN/Password security mechanism is compatible for e-applications on mobile device

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 46 | 9.7 | 9.7 | 9.7 |
| | Disagree | 87 | 18.3 | 18.3 | 27.9 |
| | Neither agree nor disagree | 91 | 19.1 | 19.1 | 47.1 |
| | Agree | 167 | 35.1 | 35.1 | 82.1 |
| | Strongly Agree | 85 | 17.9 | 17.9 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(b) The function of fingerprint security mechanism is compatible for e-applications on mobile device.

In table 4.30, 111 (23.3%) of the respondents agree that the function of fingerprint security mechanism is compatible for e-applications on mobile device, 48 (10.1%) of the respondents strongly agree that the function of fingerprint security mechanism is compatible for e-applications on mobile device, 177 (37.2%) of the respondents neither agree nor disagree that the function of fingerprint security mechanism is compatible for e-applications on mobile device, 86 (18.1%) of the respondents disagree that the function of fingerprint security mechanism is compatible for e-applications on mobile device and 54 (11.3%) of the respondents strongly disagree that the function of fingerprint security mechanism is compatible for e-applications on mobile device.

Table 4.30: The function of fingerprint security mechanism is compatible for e-applications on mobile device

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 54 | 11.3 | 11.3 | 11.3 |
| | Disagree | 86 | 18.1 | 18.1 | 29.4 |
| | Neither agree nor disagree | 177 | 37.2 | 37.2 | 66.6 |
| | Agree | 111 | 23.3 | 23.3 | 89.9 |
| | Strongly Agree | 48 | 10.1 | 10.1 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(c) The function of Pattern security mechanism is compatible for e-applications on mobile device.

46 (9.7%) of the respondents strongly agree that the function of Pattern security mechanism is compatible for e-applications on mobile device, 105 (22.1%) of the respondents agree that the function of Pattern security mechanism is compatible for e-applications on mobile device, 180 (37.8%) of the respondents neither agree nor disagree that the function of Pattern security mechanism is compatible for e-applications on mobile device, 88 (18.5%) of the respondents disagree that the function of Pattern security mechanism is compatible for e-applications on mobile device and 57 (12.0%) of the respondents strongly disagree that the function of Pattern security mechanism is compatible for e-applications on mobile device; see table 4.31 below:

Table 4.31: The function of Pattern is compatible for e-applications on mobile device

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 57 | 12.0 | 12.0 | 12.0 |
| | Disagree | 88 | 18.5 | 18.5 | 30.5 |
| | Neither agree nor disagree | 180 | 37.8 | 37.8 | 68.3 |
| | Agree | 105 | 22.1 | 22.1 | 90.3 |
| | Strongly Agree | 46 | 9.7 | 9.7 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(viii) Complexity of security mechanisms

(a) Using PIN/Password security mechanism is less complex.

53 (11.1%) of the respondents strongly agree that using PIN/Password security mechanism is less complex, 116 (24.2%) of the respondents agree that using PIN/Password security mechanism is less complex, 177 (37.2%) of the respondents neither agree nor disagree that using PIN/Password security mechanism is less complex, 81 (17.0%) of the respondents disagree that using PIN/Password security mechanism is less complex and 49 (10.3%) of the respondents strongly disagree that using PIN/Password security mechanism is less complex; see table 4.32 below:

Table 4.32: Using PIN/Password security mechanism is less complex

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 49 | 10.3 | 10.3 | 10.3 |
| | Disagree | 81 | 17.0 | 17.0 | 27.3 |
| | Neither agree nor disagree | 177 | 37.2 | 37.2 | 64.5 |
| | Agree | 116 | 24.4 | 24.4 | 88.9 |
| | Strongly Agree | 53 | 11.1 | 11.1 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(b) Using Fingerprint security mechanism is less complex.

82 (17.2%) of the respondents strongly agree that using fingerprint security mechanism is less complex, 161 (33.8%) of the respondents agree that using fingerprint security mechanism is less complex, 129 (27.1%) of the respondents neither agree nor disagree that using fingerprint security mechanism is less complex, 72 (15.1%) of the respondents disagree that using fingerprint security mechanism is less complex and 32 (6.7%) of the respondents strongly disagree that using fingerprint security mechanism is less complex; see table 4.33 below:

Table 4.323: Using Fingerprint security mechanism is less complex

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 32 | 6.7 | 6.7 | 6.7 |
| | Disagree | 72 | 15.1 | 15.1 | 21.8 |
| | Neither agree nor disagree | 129 | 27.1 | 27.1 | 48.9 |
| | Agree | 161 | 33.8 | 33.8 | 82.8 |
| | Strongly Agree | 82 | 17.2 | 17.2 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(c) Using Pattern security mechanisms is less complex.

88 (18.5%) of the respondents strongly agree that using Pattern security mechanisms is less complex, 186 (39.1%) of the respondents agree that using Pattern security mechanisms is less complex, 96 (20.2%) of the respondents neither agree nor disagree that using Pattern security mechanisms is less complex, 77 (16.2%) of the respondents disagree that using Pattern security mechanisms is less complex and 29 (6.1%) of the respondents strongly disagree that using Pattern security mechanisms is less complex; see table 4.34 below:

Table 4.34: Using Pattern security mechanisms is less complex

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 29 | 6.1 | 6.1 | 6.1 |
| | Disagree | 77 | 16.2 | 16.2 | 22.3 |
| | Neither agree nor disagree | 96 | 20.2 | 20.2 | 42.4 |
| | Agree | 186 | 39.1 | 39.1 | 81.5 |
| | Strongly Agree | 88 | 18.5 | 18.5 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

(d) Using combination of password and fingerprint security mechanism is less complex.

36 (7.6%) of the respondents strongly agree that using combination of password and fingerprint security mechanism is less complex, 66 (13.9%) of the respondents agree that using combination of password and fingerprint security mechanism is less complex, 133 (27.9%) of the respondents neither agree nor disagree that using combination of password and fingerprint

security mechanism is less complex, 165 (34.7%) of the respondents disagree that using combination of password and fingerprint security mechanism is less complex and 76 (16.0%) of the respondents strongly disagree that using combination of password and fingerprint security mechanism is less complex; see table 4.35 below:

Table 4.35: Using combination of password and fingerprint security mechanism is less complex

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|----------------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 36 | 7.6 | 7.6 | 7.6 |
| | Disagree | 66 | 13.9 | 13.9 | 21.4 |
| | Neither agree nor disagree | 133 | 27.9 | 27.9 | 49.4 |
| | Agree | 165 | 34.7 | 34.7 | 84.0 |
| | Strongly Agree | 76 | 16.0 | 16.0 | 100.0 |
| | Total | 476 | 100.0 | 100.0 | |

4.6 RELATIONSHIPS BETWEEN THE VARIABLES

Based on the research objective, to evaluate the proposed framework and establish if there is any relationship between the technology adoption factors, Pearson correlation coefficient was conducted to establish the relationships between the factors. Findings from table 4.36 revealed that there was a significant positive correlation between all eight (8) factors for users' perceptions on the security of mobile computing for adoption of e-applications (Perceived Usefulness of security mechanisms, Perceived Ease of Use of security mechanisms, Subjective norm on security mechanisms, Relative Advantage of security mechanisms, Aesthetics of security mechanisms interface, Compatibility of security mechanisms, Complexity of security mechanisms and Intention to adopt e-applications). In this study the correlation coefficients range from moderate ($r=0.595$) to very strong ($r=0.840$).

Table 4.36: Correlation Coefficient

| | PU | PEOU | AEST | RAD | SN | COMPL | COM | ITA |
|--|--------|--------|--------|--------|--------|--------|--------|-----|
| Perceived Usefulness of security mechanisms | 1 | | | | | | | |
| Perceived Ease Of Use security mechanisms | .595** | 1 | | | | | | |
| Aesthetics of security mechanisms interface | .833** | .603** | 1 | | | | | |
| Relative Advantage of security mechanisms | .757** | .638** | .754** | 1 | | | | |
| Subjective norm on security mechanisms | .647** | .655** | .666** | .736** | 1 | | | |
| Complexity of security mechanisms | .741** | .609** | .795** | .737** | .840** | 1 | | |
| Compatibility of security mechanisms | .597** | .508** | .600** | .637** | .590** | .710** | 1 | |
| Intention to adopt e-applications | .649** | .613** | .693** | .731** | .822** | .779** | .763** | 1 |
| **. Correlation is significant at the 0.01 level | | | | | | | | |

The relationship between the factors derived from DOI and TAM2 of e-applications is supported by the data given in figure 4.1. The results shown are consistent with the previous finding within Chin and Lin's (2015) study in predicting users' intention through the perceived usefulness and perceived ease of use. As shown in figure 4.1, all of the relationships between PU ($r=.649^{**}$, $p<0.001$), PEOU($r=.613^{**}$, $p<0.001$) and ITA were positive and statistically moderately correlated. Relationship between SN($r=.822^{**}$, $p<0.001$) and ITA was positive and statistically strongly correlated.

The results also showed that relationship between PEOU($r=.595^{**}$, $p<0.001$), SN($r=.647$, $p<0.001^{**}$), COM($r=.597^{**}$, $p<0.001$) and PU were positive and statistically moderately correlated. Additionally, the relationship between RAD($r=.757^{**}$, $p<0.001$), AEST($r=.833^{**}$, $p<0.001$), COMPL($r=.741^{**}$, $p<0.001$) and PU were positive and statistically strong correlated. Furthermore, results showed that all of the relationships between SN($r=.655^{**}$, $p<0.001$), RAD($r=.638^{**}$, $p<0.001$), COM($r=.508^{**}$, $p<0.001$), COMPL($r=.609^{**}$, $p<0.001$), AEST($r=.603^{**}$, $p<0.001$) and PEOU were positive and statistically moderately correlated.

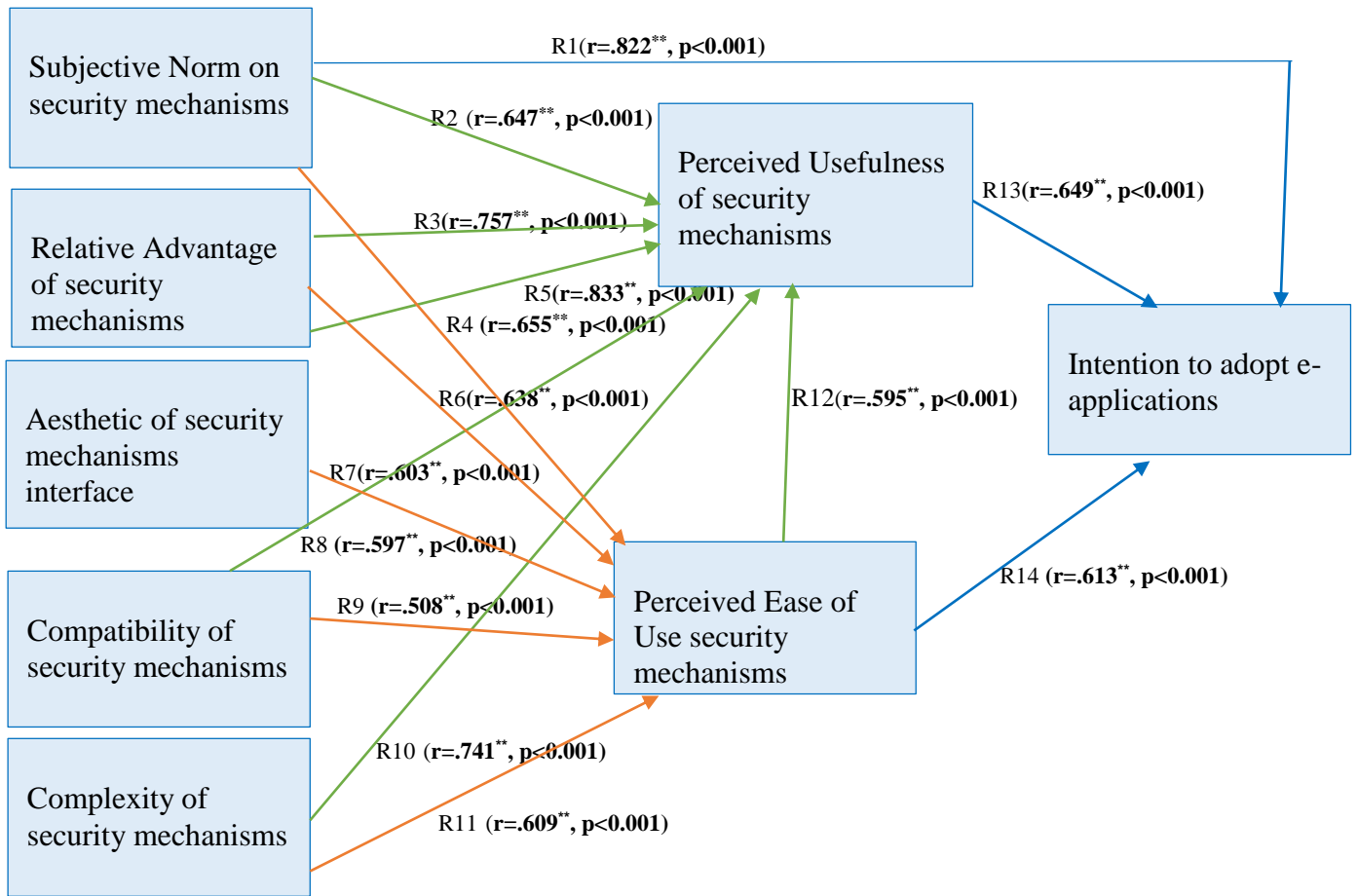


Figure 4.1: Correlation Coefficient

4.7 HYPOTHESES TESTING RESULTS

As shown in table 4.37, the strength of the relationship between related constructs were evaluated by checking the significance of path coefficient (β) and the squared R (R^2) coefficient of determination. The results shown is consistent with previous finding within (Chin & Lin's (2015), Alwan & Al-zu'bi (2016b), Olasina (2015)) study in predicting users' intention through the perceived usefulness and perceived ease of use. Perceived usefulness of security mechanisms with a path coefficient of $\beta=.178$, $p<0.001$, perceived ease of use of security mechanisms with a path coefficient of $\beta=.078$, $p<0.05$, subjective norm on security mechanisms with a path coefficient of $\beta=.655$, $p<0.001$ have a positive influence on intention to adopt e-applications and thus support H1, H2 and H4. Furthermore, these variables explained $R^2=0.702$ coefficient of determination on intention to adopt e-applications. These results are in support with the findings within the previous studies (Khairi & Baridwan (2015), Santouridis & Kyritsi (2014), Goswami (2017), Widyawani & Santosa (2017)).

Furthermore, other findings indicated that Subjective norm on security mechanisms with a path coefficient of $\beta=.409$, $p<0.001$, Relative Advantage of security mechanisms with a path coefficient of $\beta=.240$, $p<0.001$ and Aesthetics of security mechanisms interface with a path coefficient of $\beta=.530$, $p<0.001$ has a positive influence on Perceived Usefulness of security mechanisms, and thus supports H5, H7 and H11. The results shown is reliable with previous finding within Elkaseh et al. (2015) and Chen et al. (2016). Whereas Perceived Ease of Use of Security Mechanisms with a path coefficient of $\beta=.060$, $p>0.05$, Complexity of security mechanisms with a path coefficient of $\beta=.108$, $p>0.05$ and Compatibility of security mechanisms with a path coefficient of $\beta=.041$, $p>0.05$ has a negative influence on Perceived Usefulness of security mechanisms and these variables explained the largest $R^2=0.740$ coefficient of determination on Perceived Usefulness of security mechanisms.

Additionally, the results showed that Relative Advantage of security mechanisms with a path coefficient of $\beta=.204$, $p<0.05$, Aesthetics of security mechanisms interface with a path coefficient of $\beta=.222$, $p<0.001$ and Compatibility of security mechanisms with a path coefficient of $\beta=.095$, $p<0.05$ has a positive influence on Perceived Ease of Use of security mechanisms and thus supports H8, H12 and H10. The results shown is consistent with previous finding within Gangwar and Date (2015). However Subjective norm on security mechanisms with a path coefficient of $\beta=-.036$, $p>0.05$ and Complexity of security mechanisms with a path coefficient of $\beta=-.129$, $p>0.05$ has a negative influence on Perceived Ease of Use of security mechanisms, which explains $R^2=0.501$ coefficient of determination on Perceived Ease of Use security mechanisms. However, out of the fourteen (14) proposed hypothesis, five (5) were not supported (H3, H13, H9, H6 and H14) and the rest were supported.

Table 4.37: Hypotheses test results

| Criterion | Predictor | Hypothesis | Standardized Coefficient | | | Results |
|--|--|------------|--------------------------|--------|---------|-----------|
| | | | Beta | t | Sig. | |
| Intention to adopt e-applications | <ul style="list-style-type: none"> Perceived Usefulness of security mechanisms | H1 | .178 | 5.151 | .000*** | Supported |
| | <ul style="list-style-type: none"> Perceived Ease of Use security mechanisms | H2 | .078 | 2.253 | .025* | Supported |
| | <ul style="list-style-type: none"> Subjective norm on security mechanisms | H4 | .655 | 17.833 | .000*** | Supported |
| Perceived Usefulness of security mechanisms | <ul style="list-style-type: none"> Perceived Ease of Use of security mechanisms | H3 | .060 | 1.804 | .072 | Rejected |
| | <ul style="list-style-type: none"> Subjective norm security mechanisms | H5 | .409 | 6.344 | .000*** | Supported |
| | <ul style="list-style-type: none"> Relative Advantage of security mechanisms | H7 | .240 | 5.633 | .000*** | Supported |
| | <ul style="list-style-type: none"> Complexity of security mechanisms | H13 | .108 | 1.863 | .063 | Rejected |
| | <ul style="list-style-type: none"> Aesthetic security mechanisms interface | H11 | .530 | 12.120 | .000*** | Supported |
| | <ul style="list-style-type: none"> Compatibility of security mechanisms | H9 | .041 | 1.178 | .240 | Rejected |
| Perceived Ease of Use of security mechanisms | <ul style="list-style-type: none"> Subjective norm on security mechanisms | H6 | -.036 | -.750 | .454 | Rejected |
| | <ul style="list-style-type: none"> Relative Advantage of security mechanisms | H8 | .204 | 3.496 | .001** | Supported |
| | <ul style="list-style-type: none"> Complexity of security mechanisms | H14 | -.129 | -1.610 | .108 | Rejected |
| | <ul style="list-style-type: none"> Aesthetics of security mechanisms interface | H12 | .222 | 3.724 | .000*** | Supported |

| | | | | | | |
|--|--|-----|------|-------|-------|-----------|
| | <ul style="list-style-type: none"> Compatibility of security mechanisms | H10 | .095 | 1.987 | .047* | Supported |
|--|--|-----|------|-------|-------|-----------|

Sig. (*) $p < .05$, (**) $p < .01$, (***) $p < .001$.

4.8 CONFIRMED RESEARCH MODEL

First hypothesis (H1) with a correlation coefficient of .178 is confirmed and a significance level of .000 is supported. This means when users become aware of Perceived of Usefulness of security mechanisms, there would be a high chance to adopt e-applications.

The second hypothesis (H2) with a correlation coefficient of .078 is confirmed and a significance level of .025 is supported. Thus, Perceived Ease of Use of security mechanisms helps better implementation and effectiveness of security mechanisms on e-applications.

The fourth hypothesis (H4) with a correlation coefficient of .655 and a significance level of .000 is supported. Therefore the higher the Subjective norm on security mechanisms, the likelihood for them to have intentions to adopt e-applications increases.

The fifth (H5) with the correlation coefficient of .409 is confirmed and a significance level of .000 is supported. So, when users get highly influenced to use security mechanisms by others, there would be a high chance to see the Perceived usefulness of security mechanisms.

The seventh (H7) with the correlation coefficient of .240 is confirmed and a significance level of .000 is supported. Hence, the more users see the Relative Advantage of security mechanisms, the higher the chance to see the Perceived usefulness of security mechanisms.

The eighth (H8) with the correlation coefficient of .204 is confirmed and a significance level of .001 is supported. Therefore, the more users see the Relative Advantage of security mechanisms, the higher the chance to see the Perceived Ease of Use of security mechanisms.

The tenth (H10) with the correlation coefficient of .095 is confirmed and a significance level of .047 is supported. Accordingly, the higher the Compatibility of security mechanisms the higher the rate for users to see the Perceived Ease of Use of security mechanisms.

The eleventh (H11) with the correlation coefficient of .530 is confirmed and a significance level of .000 is supported. As a result, the greater the beauty and quality (Aesthetic) of security

mechanisms interface, the higher the chance users tend to see the Perceived Usefulness of security mechanisms.

The twelfth (H12) with the correlation coefficient of .222 is confirmed and a significance level of .000 is supported. Consequently, the higher the rate of the beauty and quality (Aesthetic) of security mechanisms Interface, the higher the chance for users to see the Perceived Ease of Use of security mechanisms. See figure 4.2 below for summarized confirmed proposed research model.

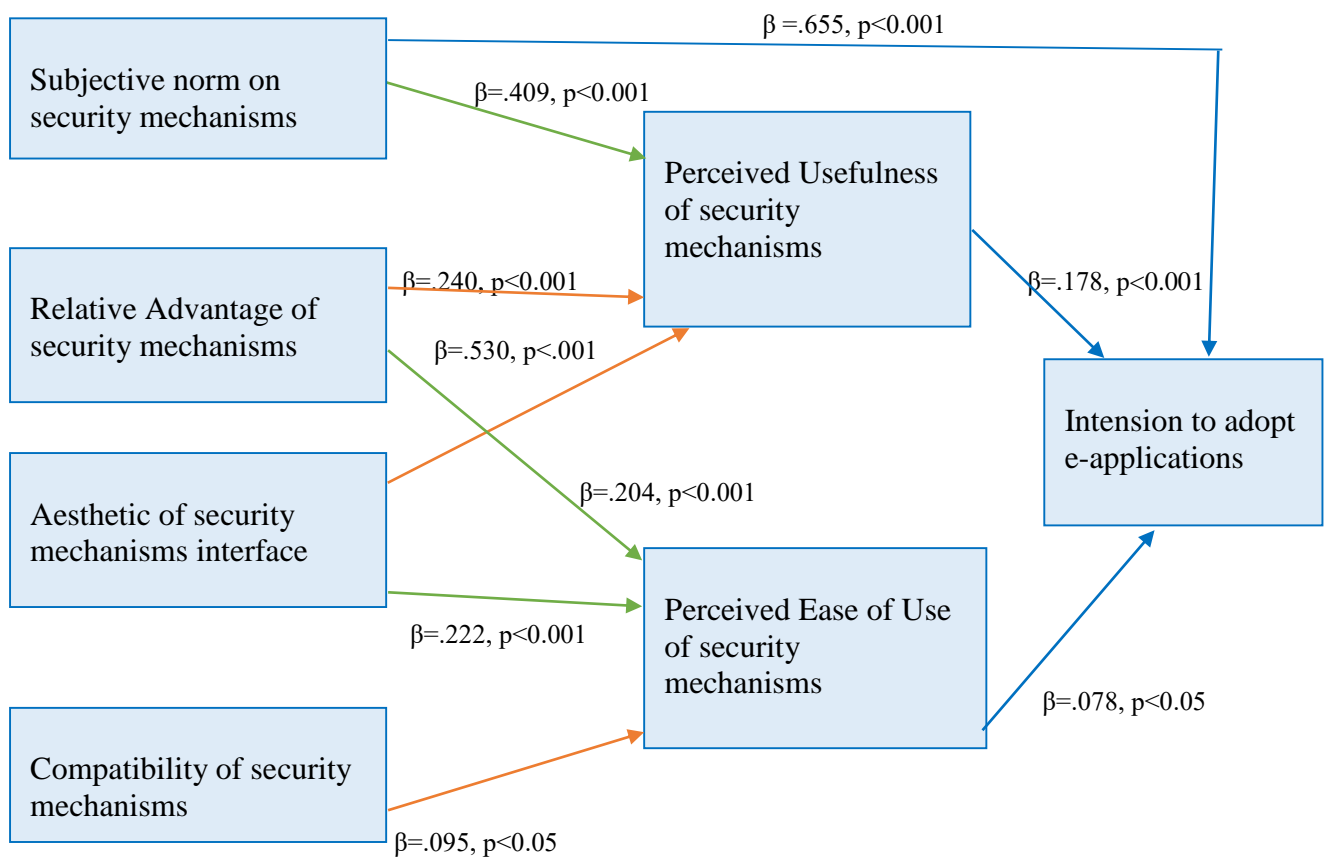


Figure 4.2: Confirmed Proposed Research Model

4.9 CHAPTER SUMMARY

This chapter has presented and analysed the data gathered and discussed the statistical results of the study. Although 83.2% of the respondents are black and fall between 26-35 years old, with high education level of diplomas and degrees, also the dominant participants are female. It is evident that the participants perceive the Aesthetic of the security mechanisms interface Perceived Usefulness of security mechanisms and Perceived Ease of Use of security

mechanisms and also clearly structured and simple. When it comes to combination of PIN and fingerprint security mechanisms participants agree that it is less complex and more advantageous to increase security for e-applications.

A Pearson correlation analysis was conducted to establish the relationships between the users' perceptions on security of mobile computing for adoption of e-applications factors and the results showed that all factors are correlated. In addition, the degree of path coefficient between the factors were also conducted to determine which factors influence the perceived usefulness of security mechanisms, perceived ease of use of security mechanisms and intention to adopt e-applications. The results demonstrate the link between various factors (Subjective norm on security mechanisms, Relative Advantage of security mechanisms, Aesthetic of security mechanisms, Compatibility of security mechanisms, Perceived Ease of Use of security mechanisms, Intention to adopt e-applications and Perceived Usefulness of security mechanisms). In the next chapter, summary, conclusions and recommendations are drawn based on the results discussed in this chapter.

CHAPTER 5: CONCLUSION AND RECOMMENDATION

5.1 INTRODUCTION

In the previous chapter, the results of the study were tabled and also presented in figures. The findings of the study were discussed in detail. The significance of the study in the context of e-applications adoption together with its security mechanisms was examined. This chapter provides study conclusions together with the recommendations drawn from the study and possible ways for future research are mentioned.

5.2 CONCLUSIONS

The overriding purpose of this study was to investigate the users' perceptions on the security of mobile computing for adoption of e-applications in South Africa. This study has applied the research model derived from DOI and TAM2 in order to accomplish the study objectives and answer the research questions. This study was conducted in South Africa but not limited to one location as questionnaires were distributed online to various respondents who are based in different provinces of South Africa. It also covered the participants with various education levels, age group and technology background as South Africa accommodates diverse backgrounds. The findings from this study led the researcher to draw a number of conclusions connected to the three (3) research questions; these are observed below.

Research Question 1: What are the users' perceptions models for technology adoption?

Different technology adoption models has been explored, whereby the ideas, applications and advancement of innovation appropriation models and hypotheses in light of the literature review include diverse perspectives and interpretation. The literature review share the distinction of innovation appropriation models and theories with various hypothetical bits of knowledge, inquire about issues, factors, and measurements. The advancement of the new hypothetical research structure will rely upon various factors yet not restricted to the accompanying: the exploration issues and targets, whole investigation and the comprehension of innovation reception models and speculations in view of the accessible materials and others. What's more, such comprehension is crucial to empower the invested individuals such as understudies, scholars, government, associations, developers and businesses to relate with both the hypothesis and reasonable parts of the innovation selection models and assumptions.

Research Question 2: What are the relevant factors for users' perceptions on security of mobile computing for adoption of e-applications in South Africa?

After assessing the literature review, the technology adoption model for South African residents was proposed based on Diffusion of Innovation (DOI) and Technology Adoption Model 2 (TAM2). DOI technology adoption model deals with individual perceptions and attitudes and highlights that user adoption is nothing more than a communication process, an information seeking and processing activity. Factors including Perceived Usefulness of security mechanisms, Perceived Ease of Use of security mechanisms, Subjective norm on security mechanisms, Relative Advantage of security mechanisms, Intention to adopt, Compatibility of security mechanisms and Complexity of security mechanisms are relevant factors for users' perceptions on security of mobile computing for adoption of e-application in South Africa on various levels.

Research Question 3: To what extent does the technology adoption factors correlate and influence on each other?

The findings have indicated that there is a strong positive correlation between Aesthetics of security mechanisms interface and Perceived Usefulness of security mechanisms. Similarly, there is a strong correlation between Complexity of security mechanisms and Perceived Usefulness of security mechanisms. Furthermore, there is a strong positive correlation between Relative Advantage of security mechanisms and Perceived Usefulness of security mechanisms. In addition, there is a strong positive correlation between Subjective norm of security mechanisms and Intention to adopt e-applications.

The objective results showed these factors have been tested using linear multiple regression based on the proposed research framework. The results revealed that Subjective norm on security mechanisms, Perceived Ease of Use of security mechanisms, Perceived Usefulness of security mechanisms combined are significant predictors of Intention to adopt e-applications. Subjective norm on security mechanisms strongly influences Intention to adopt e-applications, more than Perceived Usefulness of security mechanisms and Perceived Ease of Use of security mechanisms; these findings are also consistent with previous studies Fathima and Muthumani, (2015); Goswami (2017); Ahmed and Phin (2016); Santouridis and Kyritsi (2014) whereby Perceived Usefulness and Perceived Ease of Use were found to give direct and indirect influence towards adoption intention.

It is acknowledged that the Aesthetic of security mechanisms interface has a strong positive influence on Perceived Usefulness of security mechanisms and Perceived Ease of Use of security mechanisms, these findings are in support with the study conducted by Salimun (2013), Reinecke et al. (2013) and Thielsch, Engel and Hirschfeld (2015).

The years of delivering a technology product and hoping that it will be successful based on its attractiveness is long gone and service providers such as financial institutions, health sector, government sector, retail sector and education sector in particular have to be mindful of all the outer factors especially security if they are to benefit from the implementation. Furthermore, being very interested in the users' perceptions on the security of mobile computing for adoption of e-applications in South Africa has led to learning experience and also an opportunity to increase knowledge on Usefulness and Ease of Use of security mechanisms. It is hoped that these research findings will help developers and stakeholders to effectively plan and manage their introductions of self-services technologies by focusing on the critical factors that impact users' intention to use the technology.

5.3 RECOMMENDATIONS

This study establishes that the most important step to improving the adoption of e-applications in South Africa is to develop a suitable security mechanism user interface that will be compatible for all levels of users and also to have effective security mechanisms in place that will be useful and easy to use on e-applications platforms. Therefore, understanding the security mechanisms factors that influence the perceived ease of use of security mechanisms and perceived usefulness of security mechanisms to adopt e-applications, is crucial to ensuring that all age group and ethnic group users get to adopt e-applications.

To increase the adoption rate of e-applications in South Africa, users or peers should influence each other continuously. In addition, based on the findings and conclusions presented in this study the researcher recommends that because of the various security mechanisms interfaces being used in various e-applications such as e-governance, e-banking, e-commerce, e-health and e-learning, it is suggested that mobile devices retailers and manufacturers should enable multi-factor authentication by using sensors to capture biometric data such as fingerprint. This will assist or encourage users to understand the reason for the perceived usefulness of security mechanisms and perceived ease of use of security mechanisms and integrate it into their daily

lives (compatible); it is also less complex to improve the quality and beauty of security mechanisms interfaces.

Likewise, quality and effective interactive interfaces should be developed, so that users can master the innovation skills within a short period of time. Established on the research problem, the recommended security mechanisms interface will improve users' security on e-applications platforms and guarantee users for secure e-applications. Users are influenced by their social network in adopting or considering an innovation, since many users do not want to be left behind. In another way, the framework proposed and used in this study provides an ironic and prospective successful area for further research and contribution to be concerned with taking up innovation in the country.

Additionally, the researched technologies in this study are at different stages with regard to the product life cycle. Further studies could be undertaken that identify how the influence of each of these factors changes as the technology advances. This would give a clearer representation on how the adoption factors influence the use of technology at various phases as well as the adoption factors' interaction with the moderating factors at various phases. A longitudinal study would be more suitable and the evidence obtained might improve our understanding of the variances that exist.

5.4 FUTURE WORK

Since the results are obtained through the Pearson correlations analysis, variables are determined for their individual association with each other; it would be advantageous to undertake further multivariate analysis so as to consider the interaction between these variables and how they jointly influence the intention to adopt e-applications. In addition, the same research should be carried out in another setting that might produce different results by expanding the study to another part of the world. Studying their perceptions on security of mobile computing and moreover evaluating how extensively exposed other users are to these benefits might be another approach to increasing an understanding adoption. Additionally, studying of extension factors which help to improve adoption and provide the ability for implementation of security mechanisms interfaces, deserves some attention. Further research could be conducted in order to investigate if aesthetics of security mechanism interfaces does influence the intention to adopt e-applications.

REFERENCES

- ABDEKHODA, M., DEHNAD, A., MIRSAEED, S. J. G. & GAVGANI, V. Z. (2016). Factors influencing the adoption of e-learning in Tabriz University of Medical Sciences. *Medical Journal of the Islamic republic of Iran*. 30. p.1-7.
- ABDULWAHID, A. A., CLARKE, N., STENGEL, I., FURNELL, S. & REICH, C. (2015). Security, privacy and usability-a survey of users'perceptions and attitudes. *International conference on trust and privacy in digital business*. 9264. p.153-168.
- ABDURACHMAN, E. & SRIWARDININGSIH, E. (2016). The effect of the diffusion of university website innovation on student behaviour of state and private universities: a comparative study. *Pertanika J. Soc. Sci. and Hum*. 24. p.177-186.
- ABID, B. (2016). Security issues in mobile computing vs mobile cloud computing from user perspective. *International journal of scientific and engineering*. 7. p.1388-1395.
- ABOELMGED, M. G. & GEBBA, T. R. (2013). Mobile banking adoption: an examination of technology acceptance model and theory of planned behavior. *International journal of business research and development*. 2. p.35-50.
- ABRAHAO, R. D. S., MORIGUCHI, S., NAOMI & ANDRADE, D. F. (2016). Intention of adoption of mobile payment: an analysis in the light of the unified theory of acceptance and use of technology(UTAUT). *RAI revista de administracaoe Inovacao*. 13. p.221-230.
- ABU-ASSI, H. A., AL-DMOUR, H. H. & ZU'BI, M. (2014). Determinants of internet banking adoption in Jordan. *International Journal of Business and Management*. 9. p.169.
- ADETOBA, B. T., AWODELE, O. & KUYORO, S. O. (2016). E-learning security issues and challenges: A review. *Journal of scientific research and studies*. 3. p.96-100.
- AHLAN, A. R. & AHMAD, B. I. E. (2015). An overview of patient acceptance of health information technology in developing countries: a review and conceptual model. *International journal of information systems and project management*. 3. p.29-48.
- AHMAD, N. N., TARMIDI, M., RAIDZWAN, I. U., HAMID, M. A. & RONI, M. A. (2014). The application of unified theory of acceptance and use of technology (UTAUT) for predicting the usage of e-zakat online system. *International journal of science and research (IJSR)*. 3. p.63-66.
- AHMED, E. & PHIN, G. (2016). Factors influencing the adoption of internet banking in Malaysia. *Journal of Internet Banking and Commerce*. 21. p.1.
- AILA, F. & OMBOK, B. (2015). Validating Measures in Business Research: Practical Implications. *International Journal of Science and Engineering*. 1. p.11-19.
- AIZSTRAUTA, D., GINTERS, E. & EROLES, P. M.-A. (2014). Applying theory of diffusion of innovations to evaluate technology acceptance and sustainability Procedia computer science: ICTE in regional development, December 2014 Valmiera, Latvia. p.69-77.

- AJZEN, I. (1985). From intentions to actions: A theory of planned behavior. *Action control*. Springer.
- AKHAVAN, P., HOSSEINI, S. M., ABBASI, M. & MANTEGHI, M. (2015). Knowledge-sharing determinants, behaviors, and innovative work behaviors: An integrated theoretical view and empirical examination. *Aslib Journal of Information Management*. 67. p.562-591.
- AL-GHAITH, W. (2015). Applying the technology acceptance model to understand social networking sites (SNS) usage: impact of perceived social capital. *International journal of computer science and information technology (IJCSIT)*. 7. p.105-117.
- AL-MAMARY, Y. H., AL-NASHMI, M. & HASSAN, Y. A. G. (2016). A critical review of models and theories in field of individual acceptance of technology. *International journal of hybrid information technology*. 9. p.143-158.
- AL-SHBIEL, S. O. & AHMAD, M. A. (2016). A theoretical discussion of electronic banking in Jordan by integrating technology acceptance model and theory of planned behaviour. *International journal of academic research in accounting, finance and management science*. 6. p.272-284.
- ALHUSSAIN, T., ALGHAMDI, R., ALKHALAF, S. & ALFARRAJ, O. (2013). Users' perceptions of mobile phone security: a survey study in the kingdom of Saudi Arabia. *International journal of computer theory and engineering*. 5. p.793-796.
- ALOMARY, A. & WOOLLARD, J. (2015). How is technology accepted by users? a review of technology acceptance models and theories. Proceedings of the IRES 17th international conference 21 November 2015 London, United Kingdom. 1-4.
- ALOTAIBI, E. F. & ALBAR, A. M. (2016). Mobile computing security :issues and requirements. *Journal of advances in information technology*. 7. p.8-12.
- ALSAIARI, H., PAPADAKI, M., DOWLAND, P. S. & FURNELL, S. M. (2014). Alternative Graphical authentication for online banking environment. *Proceedings of the eighth international symposium on human aspects of information security and assurance (HAISA 2014)*. p.122-136.
- ALSAMYDAI, M. J. (2014). Adaptation of the technology acceptance model (TAM) to the use of mobile banking services. *International review of management and business research*. 3. p.2016-2028.
- ALSAYED, A. O. & BILGRAMI, A. L. (2017). E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. *International Journal of Emerging Technology and advanced engineering*. 7. p.109-115.
- ALWAHAISHI, S. & SNÁSEL, V. (2013). Acceptance and use of information and communications technology: a UTAUT and flow based theoretical model. *Journal of technology management & innovation*. 8. p.61-73.
- ALWAN, H. A. & AL-ZU'BI, A. (2016a). Determinants of internet banking adoption among customers of commercial banks: an empirical study in the Jordanian banking sector. *International Journal of business management*. 11. p.95-104.

- ALWAN, H. A. & AL-ZU'BI, A. I. (2016b). Determinants of internet banking adoption among customers of commercial banks: An empirical study in the Jordanian banking sector. *International journal of business and management*. 11. p.95-104.
- AMEME, B. K. (2015). The impact of customer demographic variables on the adoption and use of internet banking in developing economies. *Journal of internet banking and commerce*. 20. p.1204-5357.
- ANGELACHE, C. D. & SACLA, C. (2016). Multiple linear regression used to analyse the correlation between GDP and some variables *Romanian statistical review-supplement nr.9/2016*. p.94-99.
- ANGELES, R. (2014). Using the technology-organization environment framework for analyzing nike's "considered index" green initiative, a decision support system-driven system. *Journal of management and sustainability*. 4. p.96-113.
- ANTWI, S. K. & HAMZA, K. (2015). Qualitative and quantitative research paradigms in business research: A philosophical reflection. *European Journal of Business and Management*. 7. p.217-225.
- ANWAR, M. & BRUSILOVSKY, P. (2017). Privacy and Territoriality issues in an online social learning portal. *International Journal of information security and privacy*. 11. p.1-4.
- ARKORFUL, V. & ABAIDOO, N. (2014). The role of e-learning, the advantages and disadvantages of its adoption in higher education. *International journal of education and research*. 2. p.1-14.
- ASMAA, K. & NAJIB, E. K. (2016). E-learning systems risks and their security. *INternational journal of computer science and information security (IJCSIS)*. 14. p.193-200.
- AZETA, A. A. & IBUKUN, E. (2016). Applying diffusion of innovation (DOI) theory to mobile learning for quality education. *International journal of multimedia and ubiquitous engineering*. 11. p.147-156.
- BAGARUKAYO, E. & KALEMA, B. (2015). Evaluation of e-learning usage in South African universities: A critical review. *International Journal of education and development using information and communication technology (IJEDICT)*. 11. p.168-183.
- BAGDASARIAN, H. (2015). Difference Between Security and Protection [Online]. Available: <https://www.linkedin.com/pulse/difference-between-security-protection-henry-bagdasarian/> [Accessed 27 May 2017]
- BALWIR, S. J. & KONDEKAR, M., DR. (2015). Security Issues in Mobile Computing. *International Journal of Computer Science and Mobile Applications*. 3. p.31-40.
- BANDARA, I., LORAS, F. & MAHER, K. (2014). Cyber security concerns in e-learning education. Proceedings of ICERI2014 Conference, 17th-19th November 2014 Seville, Spain. 0728-0734.

- BANOOBHAI-ANWAR, I. & KEATING, K. (2016). An investigation into e-commerce in hospitality: A Cape Town study.
- BARUA, A. (2013). Methods for decision-making in survey questionnaires based on Likert scale. *Journal of Asian Scientific Research*. 3. p.35.
- BASKARAN, S., MA Kumari, N., RASID, S. Z. A. & RIZAL, A. M. (2017). A Proposed Framework of Academic Staff Up-Take in Integrating E-Learning in the Education Delivery. *International Journal of Academic Research in Business and Social Sciences*. 7. p.345-355.
- BEAUDIN, S., LEVY, Y., PARRISH, J. & DANET, T. (2016). An empirical study of authentication methods to secure e-learning system activities against impersonation fraud. *Online journal of applied knowledge management*. 4. p.42-61.
- BELAS, J., KORAU, M., KOMBO, F. & KORAU, A. (2016). Electronic banking security and customer satisfaction in commercial banks. *Journal of security and sustainability issues*. 5. p.412-422.
- BILAN, Y. (2013). Sustainable development of a company: Building of new level relationship with the consumers of XXI. Century. *Anfiteatru Economic*. 15. p.687-701.
- BILIC, D. G. (2017). Mobile security: the reality of malware augmented. *Trends 2017: security held ransom*. p.15-21.
- BOSHKOSKA, M. & SOTIROSKI, K. (2018). An empirical study of customer usage and satisfaction with e-banking services in the Republic of Macedonia. *Croatian Review of Economic, Business and Social Statistics (CREBSS)*. 4. p. 1-13
- BUC, S. & DIVJAK, B. (2015). Innovation diffusion model in higher education: case study of e-learning diffusion. *International conference of e-learning*. p.205-207.
- BUC, S. & DIVJAK, B. (2016). Environmental factors in the diffusion of innovation model: diffusion of e-learning in a higher education institution. Central european conference on information and intelligent systems, 21-23 September 2016 Varazdin, Croatia. p.100-250.
- BUSHRA, M. E. E. (2016). The impact of information security management for e-banks performance in Kingdom of Sudi Arabia. *International Journal of engineering sciences and research technology*. 5. p.266-271.
- BUSINESSTECH. (2017). *Battle of the banks: How SA's big five banks compare* [Online]. BusinessTech. Available: <https://businesstech.co.za/news/banking> [Accessed 2 July 2017]
- BWALYA, K. J. & MUTULA, S. (2016). A conceptual framework for e-government development in resource-constrained countries: The case of Zambia. *Information Development*. 32. p.1183-1198.
- CHAN-KOOK, P., HYUN-JAE, K. & YANG-SOO, K. (2014). A study of factors enhancing smart grid consumer engagement. *Energy policy*. 72. p.211-218.

- CHANGCHIT, C. (2014). Students' perceptions of cloud computing. *Issues in Information Systems*. 15. p.312-322.
- CHEN, L. & WANG, R. (2016). Trust development and transfer from electronic commerce to social commerce: an empirical investigation. *American journal of industrial and business management*. 6. p.568-576.
- CHEN, M.-C., CHEN, S.-S. & YEH, H.-M. (2016). The key factors influencing internet finances services satisfaction: an empirical study in Taiwan. *American journal of industrial and business management*. 6. p.748-762.
- CHEN, Y. & DAI, H. (2014). Do innovators concern less about security and value new technologies more? a case of mobile commerce. *Journal of information technology management*. xxv. p.13-26.
- CHEN, Y. & HE, W. (2013). Security risks and protection in online learning: A survey. *The international review of research in open and distance learning*. 14. p.109-127.
- CHIN, J. & LIN, S.-C. (2015). Investigating users' perspectives in building energy management system with an extension of technology acceptance model: a case study in indonesian manufacturing companies. *Procedia Comput. Sci*. 72. p.31-39.
- CHIN, J. & LIN, S.-C. (2016). A behavioral model of managerial perspectives regarding technology acceptance in building energy management systems. *Sustainability*. 8. p.1-13.
- CHOTO, P., TENGEH, R. K. & IWU, C. G. (2014). Daring to survive or to grow? the growth aspirations and challenges of survivalist entrepreneurs in South Africa. *Environmental economics*. 5. p.93-101.
- CHOUBEY, J. & CHOUBEY, B. (2013). Secure user authentication in internet banking: a qualitative survey. *International journal of innovation management and technology*. 4. p.198-203.
- CHOY, L. T. (2014). The strengths and weaknesses of research methodology: Comparison and complimentary between qualitative and quantitative approaches. *IOSR Journal of Humanities and Social Science*. 19. p.99-104.
- CHUCHUEN, C. (2016). The Perception of Mobile Banking Adoption: The Study of Behavioral, Security, and Trust in Thailand. *International Journal of Social Science and Humanity*. 6. p.547-550.
- CHUI-YU, C., CHEN, S. & CHUN-LIANG, C. (2017). An international perspective of TOE framework and innovation diffusion in broadband mobile applications adoption by enterprises. *International journal of management, economics and social sciences*. 6. p.14-39.
- CIJINA, K. & SAARTJIE, G. S. (2016). Evaluating e-learning readiness and effectiveness at a parastatal. South Africa international conference on educational technologies 24-26 April 2016 Manhattan Hotel, Pretoria, South Africa. p.12-21.

- CRAWFORD, H., RENAUD, K. & STORER, T. (2013). A framework for continuous transparent mobile device authentication. *Comput. Secur.* 39. p.127-136.
- DAI, N. H. P., ANDRAS, K. & ZOLTAN, R. (2016). E-learning security risks and counter measures. *Engineering research and solutions in ICT.* 1. p.17-25.
- DAI, Z. (2015). Factors affecting university students intention to adopt e-learning systems: a case study in Jiujiang University. *International Journal of Networking and Virtual organizations.* 15. p.102-119.
- DAMASEVICIUS, R., MASKELIUNAS, R. & VENCKAUSKAS, A. (2016). Smartphone user identity verification using gait characteristics. *Symmetry.* 8. p.1-20.
- DAVIS, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *Mis Q.* 13. p.319-340.
- DAVIS, F. D. & BAGOZZI, R. P. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management science.* 35. p.982-1003.
- DAVIS JR, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: Theory and results.* Massachusetts Institute of Technology.
- DE VEER, A. J., PEETERS, J. M., BRABERS, A. E., SCHELLEVIS, F. G., RADEMAKERS, J. J. J. & FRANCKE, A. L. (2015). Determinants of the intention to use e-Health by community dwelling older people. *BMC health services research.* 15. p.103.
- DEGERLI, A., AYTEKIN, C. & DEGERLI, B. (2015). Analyzing information technology status and networked readiness index in context of diffusion of innovations theory. *Procedia social and behavioral sciences.* 195. p.1553-1562.
- DHINGRA, N. (2014). Challenges, Limitation and security issues on mobile computing. *International journal of current engineering and technology.* 4. p.3459-3462.
- DICKSON, B. (2016). *5 authentication methods putting passwords to shame.* [Online]. Available: [https:// thenextweb.com/insider/2016/03/31/5-technologies-will-flip-world-authentication-head](https://thenextweb.com/insider/2016/03/31/5-technologies-will-flip-world-authentication-head) [Accessed 17 August 2018]
- DRIGĂ, I., ISAC, C. (2014). E-banking services– Features, Challenges and Benefits. *Annals of the University of Petrosani, Economics.* 14. p. 49-58.
- DUDHE, P. D. & RAMTEKE, P. L. PROF. (2014). Mobile computing with wireless LAN and its modes Ad Hoc network with challenges. *International journal of computer science and mobile computing.* 3. p.671-676.
- DURODOLU, O. O. (2016). Technology acceptance model as a predictor of using information system to acquire information literacy skills. *Library of philosophy and practice (e-journal).* 1450. p.1-27.

- EFFECTIVEMEASURE. (2017). *South Africa Mobile Report 2017* [Online]. Available: <https://www.effectivemeasure.com> [Accessed 15 May 2017]
- EHOMEAFFAIRS. (2017). *eChannel* [Online]. Available: <https://ehome.dha.gov.za/eChannel/> [Accessed 31 May 2017]
- ELKASEH, A. M., WONG, K. W. & FUNG, C. C. (2015). The acceptance of e-learning as a tool for teaching and learning in Libyan higher education. *IPASJ international journal of information technology (IJIT)*. 3. p.1-11.
- ERASMUS, E., ROTHMANN, S. & VAN EEDEN, C. (2015). A structural model of technology acceptance. *SA journal of Industrial psychology*. 41. p.1-12.
- ESCOBAR, V., WU, H., MORAN, S. & O'NEILL, P. (2016). SMAP Impact Analysis of Early Adopter Research-Two Case studies on the scientific and societal benefits of SMAP data. AGU Fall Meeting Abstracts, 2016.
- FATHIMA, Y. A. & MUTHUMANI, S. (2015). User acceptance of banking technology with special reference to internet banking. *Journal of Theoretical & Applied Information Technology*. 73.
- FICHTEN, C. S., AMSEL, R., JORGENSEN, M., NGUYEN, M. N., BUDD, J., HAVEL, A., LAURA KING, JORGENSEN, S. & ASUNCION, J. (2016). Theory of Planned Behavior: Sensitivity and Specificity in Predicting Graduation and DropOut among College and University Students. *International Journal of Learning, Teaching and Educational Research*. 15. p.38-52.
- FISHBEIN, M. & AJZEN, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*.
- GAJBHIYE, S., SHARMA, S. K. & AWASTHI, M. K. (2015). Application of principal components analysis for interpretation and grouping of water quality parameters. *International journal of hybrid information technology*. 8. p.89-96.
- GANGWAR, H. & DATE, H. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Journal of enterprise information management*. 8. p.1-33.
- GANGWAR, H., DATE, H. & RAMASWAMY, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Journal of Enterprise Information Management*. 28. p.107-130.
- GAUTAM, G. & YADAV, D. (2014). Sentiment analysis of twitter data using machine learning approaches and semantic analysis. Contemporary computing (IC3), 2014 seventh international conference on, 2014. IEEE. p.437-442.
- GOGTAY, N. J. & THATTE, U. M. (2017). Principles of correlation analysis. *Journal of the association of physicians of India*. 65. p.78-81.
- GOSWAMI, S. (2017). Are customers ready to use mobile technology for banking transactions? an investigation. *Journal of internet banking and commerce*. 22. p.1-13.

- GRIFFIN, P. H. (2015). Biometric knowledge extraction for multi-factor authentication and key exchange. *Procedia computer science*. 61. p.66-71.
- GUPTA, P. & DUBEY, A. (2016). E-Commerce-Study of privacy, trust and security from customer's perspective. *International Journal of computer science and mobile computing*. 5. p.224-232.
- GURITNO, R. S. & SIRINGORINGO, H. (2013). Perceived usefulness, ease of use and attitude towards onlinen shopping usefulness towards online airlines ticket purchase. *Procedia social and behavioral sciences*. p.81.
- HADI, N. U., ABDULLAH, N. & SENTOSA, I. (2016). An easy approach to exploratory factor analysis: Marketing perspective Noor Ul Hadi. *Journal of Educational and social research*. 6. p.215-223.
- HALAWEH, M. (2014). Users' perception of security for mobile communication technology. *International journal of information security and privacy (IJISP)*. 8.
- HARDIGAN, P. C., POPOVICI, L. & CARVAJAL, M. J. (2016). Response rate, response time, and economic costs of survey research: A randomized trial of practicing pharmacists. *Research in social and administrative pharmacy*. 12. p.141-148.
- HARTLEY, A. G. & FURR, R. M. (2017). A Profile-Based Framework for Factorial Similarity and the Congruence Coefficient. *Journal of Personality Assessment*. p.1-11.
- HASHEMI, S. & HASHEMI, S. Y. (2013). Cloud computing for e-learning with more emphasis on security issues. *International journal of computers, electrical, automation, control and information engineering*. 7. p.1251-1256.
- HASSAN, H., MOHDNASIR, M. H., KHAIRUDIN, N. & ADON, I. (2017). Factors influencing cloud computing adoption in small and medium enterprises. *Journal of ICT*. 16. p.21-41.
- HASSAN, R. G. & KHALIFA, O. O. (2016). E-Government-an Information Security Perspective. *International Journal of Computer Trends and Technology (IJCTT)*. 36. p.1-9.
- HERZALLAH, F. & MUKHTAR, M. (2015). The impact of internal organization factors on the adoption of e-commerce and its effect on organizational performance among palestinian small and medium enterprise. Proceedings of the International conference on e-commerce, 2015 Kuching, Sarawak, Malaysia. p.105-111.
- HOLZ, C. & BENTLEY, F. R. (2015). ON-demand biometrics: Fast cross-device authentication. CHI'16, May 07-12 2016 San Jose, CA, USA. ACM. p.1-6.
- HOTI, E. (2015). The technological, organizational and environmental framework of IS innovation adaption in small and medium enterprises. Evidence from research over the last 10 years. *International journal of business and management*. III. p.1-14.
- HSIAO, C.-H., CHANG, J.-J. & TANG, K.-Y. (2016). Exploring the influential factors in continuance usage of mobile social Apps: Satisfaction, habit, and customer value perspectives. *Telematics and Informatics*. 33. p.342-355.

- HUSSEIN, L. A. & BAHARUDIN, A. S. (2017). Factors affecting small and medium enterprises (SMEs) continuance intention to adopt e-commerce in Jordan. *International Journal of Advanced and Applied Sciences*. 4. p.110-117.
- IBUKUN, E. & DARAMOLA, O. (2015). A Systematic Literature Review of Mobile Cloud Computing. *International Journal of Multimedia and Ubiquitous Engineering*. 10. p.135-152.
- ICASA. (2016). Report on the state of the ICT Sector in South Africa. *Independent communications authority of South Africa*.
- ISABIRYE, A. K. & DLODLO, N. (2014). Perceived inhibitors of innovative e-learning teaching practice at a South African University of Technology. *Mediterranean Journal of Social Sciences*. 5. p.390-398.
- JANI, M. A., SARI, G. I. P., PRIBADI, R. C. H., NADLIFATIN, R. & PERSADA, S. F. (2015). An investigation of the influential factors on digital text voting for commercial competition: A case of Indonesia. *Procedia Computer Science*. 72. p.285-291.
- JEFFREY, D. A. (2015). *Testing the technology acceptance model 3 (TAM3) with the inclusion of change fatigue and overload, in the context of faculty from seventh day adventist universities: a revised model*. Doctor of Philosophy Dissertations, Andrews University.
- JHA, A. K. & BOSE, I. (2013). A Framework for Addressing Data Privacy Issues In E-Governance Projects. *Journal of Information Privacy and Security*. 9. p.18-33.
- JIUNN-WOEL, L. & YEN, D. C. (2014). Online shopping drivers and barriers for older adults: Age and gender differences. *Computers in Human behavior*. 37. p.133-143.
- JOSEPH, B. K. (2017). Determining Factors Influencing E-Government Development in the Developing World: A Case Study of Zambia.
- JUKSEL, I. (2015). Rogers' diffusion of innovation model in action: individual innovativeness profiles of pre-service teachers in Turkey. *Croatian Journal of Education*. 17. p.507-534.
- KALETA, A. (2014). E-learning as a diffusion of innovation in areas of the European Union. *Culture and Education*. 2. p.134-145.
- KANWAL, F. & REHMAN, M. (2014). E-learning adoption model: A case study of Pakistan. *Life Science Journal*. 11. p.78-86.
- KARAMIZADEH, S., ABDULLAH, S. M., MANAF, A. A. & HOOMAN, A. (2013). An overview of principal component analysis. *Journal of Signal and Information Processing*. 4. p.173-175.
- KARIM, R., CHOWDHURY, T. (2014). Customer satisfaction on service quality in private commercial banking sector in Bangladesh. *British Journal of Marketing Studies*. 2. p. 1-11.
- KAUR, R. (2016). E-governance: problems, challenges and prospects in India.

- KEMP, S. (2017). *Digital in 2017: Global overview* [Online]. Available: <https://thenexweb.com/> [Accessed 14 May 2017].
- KHAIRI, M. S. & BARIDWAN, Z. (2015). An empirical study on organizational acceptance accounting information systems in Sharia banking. *The International Journal of Accounting and Business Society*. 23. p.97-122.
- KHATRI, J. R. & UPADHYAY-DHUNGEL, K. (2013). Internet banking in Nepal: use and challenges. *Banking journal*. 3. p.57-77.
- KILJAN, Z. S. (2017). *Exploring, expanding and evaluating usable security in online banking*. PhD, NHL University of Applied sciences and Radboud University.
- KIM-SOON, N., AHMAD, A. R. & IBRAHIM, N. N. (2016). Theory of planned behavior: undergraduates' entrepreneurial motivation and entrepreneurship career intention at a public university. *Practice*. 501. p.615602.
- KINASH, S. (2013). Paradigms, Methodology and Methods. [Online]. Available: <https://www.bond-edu.au/prod-ext/groups/public/@pub-tls-gen/documents/genericwebdocument/bd3-012336.pdf> [Accessed 16 August 2018]
- KIVUNJA, C. (2015). Innovative methodologies for 21st century learning, teaching and assessment: A convenience sampling investigation into the use of social media technologies in higher education. *International Journal of Higher Education*. 4. p.1.
- KOLOG, E. A., SUTINEN, E., VANHALAKKA-RUOHO, M., SUHONEN, J. & ANOHAH, E. (2015). Using unified theory of acceptance and use of technology model to predict students' behavioral intention to adopt and use e-counseling in Ghana. *International Journal of Modern Education and Computer Science*. 7. p.1-11.
- KOO, C., WATTI, J. & CHUNG, N. (2014). A study of mobile and internet banking service: applying for IS success model. *Asia Pacific Journal of Information Systems*. 23. p.65-86.
- KOVAČEVIĆ, M. S., ĐUROVIĆ, M. S. (2014). Electronic banking. Law – theory and practice, 01-03/2014. p. 29-39
- KOVED, L., TREWIN, S., SWART, C., SINGH, K., CHENG, P.-C. & CHARI, S. (2013). Perceived security risks in mobile interaction. Symposium on usable privacy and security (SOUPS), July 24-26 2013. Newcastle, UK. 1-3.
- KRISHNA, P. K. & MUNIYAL, B. (2015). Security issues and challenges in mobile Computing and m-commerce. *International Journal of Computer Science & Engineering Survey*. 6. p.29-45.
- KUMARI, P., KAUR, R., HANDA, S. & KAUR, J. (2016). Biometrics authentication technique-A survey. Proceedings of international interdisciplinary conference on engineering science and management 17th-18th December 2016 Goa, India. p.369-376.

- KURNIA, S., CHOUDRIE, J., MAHBUBUR, R. M. & ALZOUGOOL, B. (2015). E-commerce technology adoption: A Malaysian grocery SME retail sector study. *Journal of Business Research*. 68. p.1906-1918.
- LAI, P. C. (2017). The literature review of technology adoption models and theories for the novelty technology. *Journal of Information Systems and Technology Management*. 14. p.21-38.
- LAL, N.A., PRASAD. S. & FARIK, M. (2016). A Review Of Authentication Methods. *International Journal Of Scientific & Technology Research*. 5. p.246-249.
- LEE, S. C., MOY, F. M. & HAIRI, N. N. (2017). Validity and reliability of the Malay version multidimensional scale of perceived social support (MSPSS-M) among teachers. *Quality of life research*. 26. p.221-227.
- LEGG, G. & MITCHELL, I. Online eLearning in Tertiary Education. 7th annual conference of computing and information technology research and education New Zealand (citrenz2016), 11-13 July 2016 Wellington, New Zealand. 1-2.
- LEKHANYA, L. M. (2016). E-Commerce as an instrument of governing SMEs' marketing strategy in an emerging economy.
- LEKSHMI B.P.S. (2018). E-banking in India. *Problems and Prospects International Journal of Current Engineering and Scientific Research (IJCESR)*.5. p.77-81.
- LEUKFELDT, E. R., KLEEMANS, E. R. & STOL, W. P. (2016). Origin, growth and criminal capabilities of cyber criminal networks: An international empirical analysis. *Crime, law and social change*.
- LEUNG, D., LO, A., FONG, L. H. N. & LAW, R. (2015). Applying the technology-organization-environment framework to explore ICT initial and continued adoption: An exploratory study of an independent hotel in Hong Kong. *Journal Tourism recreation research*. 4. p.391-406.
- LEUNG, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*. 4. p.324.
- LEYTON, D., PINO, J. A. & OCHOA, S. F. (2015). EBTAM: technology acceptance in e-business environment. *Inf. Syst. E-bus Manage*. 13. p.211-234.
- LIN, H. (2015). A meta-synthesis of empirical research on the effectiveness of computer-mediated communication in SLA. *Language Learning and Technology*. 19. p.85-117.
- LIN, P.-C., LU, H.-K. & LIU, S.-C. (2013). Towards an education behavioral intention model for e-learning systems: an extension of UTAUT. *Journal of Theoretical and Applied Information Technology*. 47. p.1120-1127.
- MAAROP, N. & OMAR, F. R. (2015). E-commerce adoption factors in Zanzibar: A descriptive study. International conference on information technology and society, 8-9 June 2015 Kuala Lumpur, Malaysia. p.12-17.

- MADHUSHI, K. & FERNANDO, M. (2016). The Impact of Corporate Brand Trust on Customer Adaptation of e-cash Mobile Payments in Sri Lanka.
- MADUKU, D. K. (2014). Customers' adoption and use of e-banking services: the South African perspective. *Banks and Bank systems*. 9. p.78-88.
- MADUKU, D. K. (2016). The effect of institutional trust on internet banking acceptance: perspectives of South African banking retail customers. *SAJEMS NS*. 19. p.533-548.
- MAHESH, P., JAYAWANT, A. & KALE, G. (2015). Smartphone security: review of attacks, detection and prevention. *International Journal of Advanced Research in Computer Science and Software Engineering*. 5. p.141-145.
- MALUFU, K., MUCHEMWA, S. & MALUFU, S. (2016). A Comparative Study of the Factors Influencing the Adoption of E-Learning by Lecturers at Universities in Bulawayo, Zimbabwe. *IOSR Journal of Research & Method in Education*. 6. p.64-73.
- MARKHASIN, A. (2017). Fundamentals of the Extremely Green, Flexible, and Profitable 5G M2M Ubiquitous Communications for Remote e-Healthcare and other Social e-Applications. *arXiv preprint arXiv:1711.06469*.
- MARNELL, J. W. & LEVY, Y. (2014). Towards a model of factors affecting resistance to using multi-method authentication systems in higher-education environments. *Information Security Education Journal*. 1. p.36-44.
- MARTINS, C., OLIVEIRA, T. & POPOVIC, A. (2014). Understanding the internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International journal of information management*.
- MATHUR, S. K. & VERMA, H. V. (2014). Significance of DOI model for adoption of cloud computing. *International Journal of Emerging Trends and Technology in Computer Science (IJETTCS)*. 3. p.228-232.
- MAUPA, H. S. E., PROF (2014). Impact of e-commerce toward Indonesian silk industry: the changing value chain of small medium enterprise in South Sulawesi municipalities. *International Journal of Managing Value and Supply Chains (IJMVSC)*. 5. p.59-69.
- MAVLETOVA, A. (2013). Data quality in pc and mobile web surveys. *National Research University Higher School of Economics*. 31. p.725-743.
- MAWELA, T., OCHARA, N. M. & TWINOMURINZI, H. (2017). E-Government implementation: a reflection on South African municipalities. *South African Computer Journal*. 29. p.147-171.
- ME, A. (2017). Empirical analysis of retail customers' adoption of internet banking services in nigeria. *Journal of Internet Banking and Commerce*. 22.
- MICHENI, E. M. (2015). Using the technology organization environment framework for adoption and implementation of cloud computing in institutions of higher learning in Kenya. *The International Journal of Engineering and Science (IJES)*. 4. p.37-43.

- MING-CHIH, C., SHIH-SHIUNN, C., HUNG-MING, Y. & WEI-GUANG, T. (2016). The key factors influencing internet finances services satisfaction: An empirical study in Taiwan. *American Journal of Industrial and Business Management*. 6. p.748-762.
- MISHRA, A. K. & SAH, P. K. (2016). Security issues in mobile computing. *International conference on advanced computing*. College of Computing Sciences and Information Technology (CCSIT) ,Teerthanker Mahaveer University , Moradabad.
- MOHAMED, S., HAFEDH, A.-S. & BADER, A.-M.(2015). System Quality Characteristics for Selecting Mobile Learning Applications. *The Turkish Online Journal of Distance Education*. 16. p.18-27.
- MOHAMMED, M. A., ABOOBAIDER, B. M., IBRAHIM, H., ABDULLAH, H. A., ALI, M. H., JABER, M. M. & SHAWKAT, A. (2016). E-government and its Challenges in Developing Countries: Case Study Iraqi e-Government. *The Social Sciences*. 11. p.4310-4319.
- MONFARED, J. H. & DERAKHSHAN, H. (2015). e Comparison Qualitative and Quantitative Research. *Indian Journal of Fundamental and Applied Life Sciences*. 5. p.1111-1117.
- MOORE, G. C. & BENBASAT, I. (1991). Development of an instrument to measure the perception of adopting an information technology innovation. *Information Systems Research*. 2. p.192-222.
- MUSAEV, E. & YOUSOOOF, M. (2015). A review on internet banking security and privacy issues in Oman. ICIT 2015 the 7th international conference on information technology, 2015. p.1-6.
- MUTLU, S. & EFEYOGLU, I. E. (2013). Evaluation of e-mail usage by extended technology acceptance model. *International Review of Management and Marketing*. 3. p.112-121.
- MWIYA, B., CHIKUMBI, C., SHIKAPUTO, C., KABALA, E., KAULUNG'OMBE, B. & SIACHINJI, B. (2017). Examining Factors Influencing E-Banking Adoption: Evidence from Bank Customers in Zambia. *American Journal of Industrial and Business Management*. 7. p.741-759.
- MYRESTEN, E. & SETTERHALL, M. (2015). Theory of Reasoned Action and the role of external factors in organic food purchase.
- NADLIFATIN, R., LIN, S.-C., RACHMANIATI, Y. P., PERSADA, S. F. & RAZIF, M. (2016). A pro-environmental reasoned action model for measuring citizens' intentions regarding ecolabel product usage. *Sustainability*. 8. p.1165.
- NAYAK, A. & BANSODE, R. (2016).Analysis of Knowledge Based Authentication System Using Persuasive Cued Click Points. *Procedia Computer Science*. 79. p. 553 – 560.
- NDEKWA, A. G. (2015). Drivers of electronic commerce (e-commerce) among small and medium tourist enterprises (SMTES) in Tanzania. *International Journal of Science and Research (IJSR)*. 4. p.2512-2517.

- NORTH, D., JOHNSTON, K. & OPHOFF, J. (2014). The Use of Mobile Phones by South African University Students. *Issues in Informing Science and Information Technology*. 11. p.115-138.
- NYEKO, J. S. & OGENMUNGU, C. (2017). Determinants of electronic learning adoption in higher institutions of learning in Uganda: A learners' Perspective. *Global Journal of Computer Science and Technology: H Information and technology*. 17. p.7-20.
- OJO, J. S. (2014). E-governance: An imperative for sustainable grass root development in Nigeria. *Journal of Public Administration and Policy Research*. 6. p.77.
- OLASINA, G. (2015). Factors Influencing the Use of M-Banking by Academics: Case Study Sms-Based M-Banking. *The African Journal of Information Systems*. 7. p.4.
- OMBATI, R. M. & OMULO, D. (2017). Factors Impacting the Adoption of E-Commerce in Cooperatives.
- ONWUZURIKE, L. & DE CRISTOFARO, E. (2015). Danger is my middle name: Experimenting with SSL vulnerabilities in Android Apps. In proceedings of the 8th ACM conference on security and privacy in wireless and mobile networks, wisec'15, 2015 New York, NY, USA. ACM, 1-6.
- OPHOFF, J. & ROBINSON, M. Exploring end-user smartphone security awareness within a South African context. Information Security for South Africa (ISSA), 2014, 2014. IEEE, 1-7.
- OPPERMANN, D. (2016). Virtual attacks and the problem of responsibility: the case of China and Russia. *Carta Internacional*. 5. p.11-25.
- OSMAN, Y. (2017). Implementation of E-learning in The University of Gezira Barriers and Opportunities. *Educational Science and Research*. 1. p.24-35.
- OSUBOR, V. O. & CHIEMEKE, S. C. (2015). The impacts of information culture of e-learning innovation adoption in learning institutions in Nigeria. *African Journal of Computing and ICT*. 8. p.17-26.
- OTIENO, O. C., LIYALA, S., ODONGO, B. C. & ABEKA, S. O. (2016). Theory of reasoned action as an underpinning to technological innovation adoption studies.
- OYE, N. D., IAHAD, N. A. & RAHIM, N. A. (2014). The history of UTAUT model and its impact on ICT acceptance and usage by academics. *Education and information technologies*. 19. p.251-270.
- PADGETT, D. K. (2016). *Qualitative methods in social work research*. Sage Publications.
- PADILLA-VEGA, R., SENQUIZ-DIAZ, C. & OJEDA, A., DR (2017). Toward a conceptual framework of technology adoption: factors impacting the acceptance of the mobile technology in the international business growth. *International Journal of Scientific and Technology Research*. 6. p.81-86.

- PALLANT, Y. (2016). SPSS survival manual: A step by step guide to data analysis using SPSS program., 2016 McGraw-Hill Education, London, UK.
- PANDYA, D., NARAYAN, K. R. & THAKKAR, S. (2015). An Overview of Various Authentication Methods and Protocols. *International Journal of Computer Applications* (0975 – 8887). 131. p.25-27.
- PARK, J.-H., KIM, M.-K. & PAIK, J.-H. (2015). The factors of technology, organization and environment influencing the adoption and usage of Big data in Korean firms. *26th European regional conference of the international telecommunications society (ITS)*. Madrid, Spain.
- PATIL, A. & GAIKWAD, R. (2015). Comparative analysis of the prevention techniques of denial of service attacks in wireless sensor network. *International conference of intelligent computing, communication and convergence*. 48. p.387-393.
- PAUL, S. & SHARMA, A. (2014). Concept of wireless sensor Ad-Hoc network focusing on mobile computing. *ISTP Journal of Research in Electrical and Electronics Engineering*. p.137-146.
- PENJOR, S. & ZANDER, P.-O. (2016). Predicting virtual learning environment adoption: a case study. *The Turkish online Journal of Educational Technology*. 15. p.69-81.
- PETROVICIC, A., PETRIC, G. & MANFREDI, K. L. (2016). The effect of email invitation elements on response rate in a web survey within an online community. *Computers in Human Behavior*. 56. p.320-329.
- PIARALAL, S. K., NAIR, S. R., YAHYA, N. & KARIM, J. A. (2015). An integrated model of the likelihood and extent of adoption of green practices in small and medium sized logistics firms. *American Journal of Economics*. 5. p.251-258.
- PONTO, J. (2015). Understanding and evaluating survey research. *Journal of the Advanced Practitioner in Oncology*. 6. p.168-171.
- POORANGI, M. M., KHIN, E. W. S., NIKOONEJAD, S. & KARDEVANI, A. (2013). E-commerce adoption in Malaysian small and medium enterprises practitioner firms: A revisit on Rogers' model. *Annals of the Brazilian Academy of sciences*. 85. p.1593-1604.
- PRASANNA, N. L. & KRISHNAIAH, R. V., DR (2013). Next generation mobile computing. *International Journal of Computer Science and Mobile Computing*. 2. p.41-47.
- PRETORIUS, M. C. & CALITZ, A. P. (2014). A methodology to institutionalise user experience in provincial government. *South African Computer Journal*. 55. p.25-39.
- PRIYAMBODO, T. K., VENANT, U., IRAWAN, T. & WAAS, D. V. (2017). A Comprehensive Review of e-Government Security. *Asian Journal of Information Technology*. 16. p.282-286.
- PSANNIS, K. E., XINOALOS, S. & SIFALERAS, A. (2014). Convergence of Internet of things and mobile cloud computing. *Systems Science & Control Engineering: An Open Access Journal of Advances in Information Technology*. 2. p.476-483.

- QUINTING, A., LINS, S., SZEFER, J. & SUNYAEV, A. (2017). Advancing the adoption of a new generation of certifications-a theoretical model to explain the adoption of continuous cloud service certification by certificate authorities. *Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (W2017)*, 2017. St. Gallen, S. p.1465-1476.
- RAEISI, F. & BEHBOUDI, M. R. (2016). A study of Unified Theory of Acceptance and the Use of Technology in Iranian Organization: Case study of cement factories. *International Business Management*. 10. p.1132-1140.
- RAEISI, S. & LINGJIE, M. (2016). Factors influencing m-commerce adoption in China. *The International Journal of Business and Management*. 4. p.372-384.
- RAHAYU, R. & DAY, J. (2015). Determinant factors of e-commerce adoption by SMEs in developing country: Evidence from Indonesia. *Procedia Social and Behavioral Sciences*. 195. p.142-150.
- RAHL, S. (2017). Research Design and Methods: A systematic review of research paradigms, sampling issues and instruments development. *International Journal of Economics and Management Sciences*. 6. p.1-5.
- RAJAN, P. C. & JAYASHREE, K. (2015). A Survey of Mobile Cloud Computing for Smart Phones. *International Journal of Science, Engineering and Technology Research (IJSETR)*. 4. p.2227-2229.
- RAMAVHONA, T. C. (2014). *Factors influencing internet banking adoption in South African rural areas*. Magister Technologiae: Business information systems, Tshwane University of Technology.
- RAMAVHONA, T. C. & MOKWENA, S. (2016). Factors influencing internet banking adoption in South African rural areas. *South African Journal of Information Management*. 18. p.1-8.
- RANI, S. & RANI, S. (2014). Threats and security issues in mobile computing. *International Journal of Current Engineering and Technology*. 4. p.3546-3550.
- RAO, R. S. & IYER, L. (2016). Education as a Determinant of E-Governance Adoption: A Case Study of Telecenters of Karnataka. *Imperial Journal of Interdisciplinary Research*. 2.
- RAWASHDEH, A. (2015). Factors affecting adoption of internet banking in Jordan: Chartered accountant's perspective. *International Journal of Bank Marketing*. 33. p.510-529.
- RAZAK, L. T. (2016). The effect of security and privacy perceptions on customers' trust to accept internet banking services: An extensive of TAM" Mohammed A. Al-Sharaf, "Ruzaini A. Arsha", "Emad Abu-Shanab" and "Nabil Elayah" Faculty of computer systems and software engineering, UMP. *Journal of Engineering and Applied Sciences*. 100. p.545-552.
- REINECKE, K., YEH, T., MIRATRIX, L., MARDIKO, R., ZHAO, Y., LIU, J. & GAJOS, K. Z. (2013). Predicting users' first impressions of website aesthetics with a quantification of perceived visual complexity and colorfulness. In proceedings of the sigchi

- conference on human factors in computing systems, 2013. Paris, France. New York, NY:ACM Press. p.2049-2058.
- RIAH, G. (2015). E-learning systems based on cloud computing: a review. *Procedia Computer Science*. 62. p.352-359.
- RINDFUSS, R. R., CHOE, M. K., TSUYA, N. O., BUMPASS, L. L. & TAMAKI, E. (2015). Do low survey response rates bias results? Evidence from Japan. *Demographic Research*. 32. p.797-828.
- ROGERS, E. M. (1995). Diffusion of Innovations: modifications of a model for telecommunications. *Die Diffusion von Innovationen in der Telekommunikation*. Springer.
- ROGERS, E. M. (2003). *Diffusion of innovations*. London, Free Press.
- SABRI, S. M., SULAIMAN, R., AHMAD, A. & TANG, A. Y. (2015). A comparative study on it outsourcing models for Malaysian SMEs e-business transformation. *ARPJ Journal of Engineering and Applied Sciences*. 10:23. 2015. p.17863-17870.
- SALEH, Z. I. & MASHHOUR, A. (2014). Consumer attitude towards m-commerce: the perceived level of security and the role of trust. *Journal of Emerging Trends in Computing and Information Sciences*. 5. p.111-1157.
- SALEM, A. (2016). The Potential Advantages of Implementing e—Government as well as Factors on Such Adoption. *International Business Management*. 10. p.292-300.
- SALIMUN, C. (2013). *The relationship between visual interface aesthetics, task performance and preference*. PhD Thesis, University of Glasgow.
- SAMARADIWAKARA, G. D. M. N. & GUNAWARDENA, C. G. (2014). Comparison of existing technology acceptance theories and models to suggest a well improved theory model. *International Technical Sciences Journal*. 1. p.21-36.
- SANAEI, Z., ABOLFAZLI, S., GANI, A. & BUYYA, R. (2014). Heterogeneity in Mobile Cloud Computing: Taxonomy and Open Challenges. *IEEE Communications Surveys & Tutorials*. 16. p.369-392.
- SANRAL. (2017). *e-toll* [Online]. Available: <https://www.sanral.co.za/> [Accessed 29 May 2017]
- SANTOURIDIS, I. & KYRITSI, M. (2014). Investigating the determinants of internet banking adoption in Greece. *Procedia Economics and Finance*. 9. p.501-510.
- SARGOLZAEI, S. (2017). Developing technology acceptance models for decision making in urban management. *MOJ Civil Engineering*. 2. p.1-4.
- SARS. (2017). *SARS e-filing* [Online]. Available: <http://www.sars.gov.za> [Accessed 29 May 2017]

- SAVULESCU, C., POLKOWSKI, Z., COSMIN, D. I. & ELENA, B. C. (2015). Security in e-learning systems. *Electronics, Computers and Artificial Intelligence (ECAI)*, 2015. 7th International Conference on, 2015. IEEE, WE-19-WE-24.
- SAYED, B., TRAORE, I., WOUNGANG, I. & OBAIDAT, M. S. (2013). Biometric authentication using mouse gesture dynamics. *IEEE Systems Journal*. 7. p.262-274.
- SERB, A., DEFTA, L., IACOB, N. M. & APETREI, M. C. (2013). Information security management in e-learning. *Knowledge Horizons*. 5. p.55-59.
- SHANKAR, A. & KUMARI, P. (2016). Factors affecting mobile banking adoption behaviour in India. *Journal of Internet Banking and Commerce*. 21. p.1-24.
- SHARABATI, A.-A. A., SHAMARI, N. S., NOUR, A.-N. I., DURRA, A.-B. I. & MOGHRABI, K. M. (2016). The impact of intellectual capital on business performance in Kuwaiti telecommunication industry. *International Journal of Business Performance Management*. 17. p.428-446.
- SHARMA, B. (2016). A focus on reliability in developmental research through Cronbach's Alpha among medical, dental and paramedical professionals. *Asian Pac. J. Health Sci*. 3. p.271-278.
- SHARMA, R. & MISHRA, R. (2014). A review of evolution of theories and models of technology adoption. *IMJ*. 6. p.17-29.
- SHATAT, A. (2017). Factors affecting the adoption and usage of online services in Oman. *Journal of Internet Banking and commerce*. 22. p.1-24.
- SHENDE, P. M., SARODE, M. V. & GHONGE, M. M. (2014). A survey based on fingerprint, face and iris biometric recognition system, image quality assessment and fake biometric. *International Journal of Computer Science Engineering and Technology (IJCSET)*. 4. p.129-132.
- SHIN, S., LEE, W.-J. & ODOM, D. (2014). A comparative study of smartphone users' perception and preference towards mobile payment methods in U.S. and Korea. *The Journal of Applied Business Research*. 30. p.1365-1376.
- SHLENS, J. (2014). A tutorial on principal component analysis. *Google Research*. Mountain View, CA 94043.
- SIBANDA, M. & DONNELLY, S. (2014). The impact of e-learning on student performance: A case study of an entry-level module at a South African University. *Mediterranean Journal of Social Sciences*. 5. p.485.
- SILA, I. (2013). Factors affecting the adoption of B2B e-commerce technologies. *Electron Commer Res*. 13. p.199-236.
- SIMPSON, S. H. (2015). Creating a data analysis plan: what to consider when choosing statistics for a study. *The Canadian Journal of Hospital Pharmacy*. 68. p.311-317.

- SINGH, A., VERMA, D. & BHARTI, V. (2016). Perceived importance of different dimensions of internet banking service quality and its perceived impact on gender. *The International Journal of Business and Management*. 4. p.205-210.
- SINGH, A. S. & MASUKU, M. B. (2014). Sampling techniques and determination of sample size in applied statistics research:an overview. *International Journal of Economics, Commerce and Management*. II. p.1-22.
- SINGH, J. (2014). Review of e-commerce security challenges. *International Journal of Innovative Research in Computer and Communication Engineering*. 2. p.2850-2858.
- SINGH, S. (2016). Modernisation Challenges: Some Factors That Affect e-Government Development in South Africa. European Conference on e-Government, 2016. Academic Conferences International Limited. p.205.
- SINGHAL, Y., SINGH, S. & MATHPAL, V. (2015). Security challenges in mobile computing. *International Journal of Advanced Research in Computer Science and Technology*. 3. p.10-11.
- SKRAČIĆ, K., PALE. P. & JEREN, B. (2014). Question based user authentication in commercial environments. *Information and Communication Technology Electronics and Microelectronics (MIPRO) 2014 37th International Convention*, p. 1422-1427.
- SOH, P. C. H. & HONG, Y. H. (2014). Factors that affect the adoption of internet banking in Malaysia. *International Business Management*. 8. p.55-63.
- SRIVASTAVA, A. (2013). Mobile banking and sustainable growth. *American Journal of Economics and Business Administration*. 5. p.89-94.
- STELLENBOSCH-UNIVERSITY. (2017). *MY.Sun* [Online]. Available: <https://www.sun.ac.za/> [Accessed 28 May 2017]
- STRANIERI, S., RICCI, E. & BANTERLE, A. 2016. The Theory of Planned Behaviour and Food Choices: The Case of Sustainable pre-packed Salad. *Proceedings in Food System Dynamics*. p.209-212.
- SUGANYA, V. & SHANTHI, A. L. (2015). Mobile Cloud Computing Perspectives and Challenges. *International Journal of Innovative Research in Advanced Engineering (IJIRAE)*. 7. p.71-76.
- SULLIVAN, G. M. & ARTINO JR, A. R. (2013). Analyzing and interpreting data from Likert-type scales. *Journal of Graduate Medical Education*. 5. p.541-542.
- SUN, G. & BIN, S. (2015). High Secure Mobile Operating System Based on a New Mobile Internet Device Hardware Architecture. *International Journal of Future Generation Communication and Networking*. 8. p.127-136.
- SVILAR, A. & ZUPANČIČ, J. (2016). User experience with security elements in Internet and mobile banking. *Organizacija*. 49. p.251-260.

- TAHIR, R. (2013). Context aware mobile computing as a challenge for developers and software enginners: A review *European Scientific Journal*. 4. p.534-536.
- TANG, K.-Y. & HSIAO, C.-H. (2016). The Literature Development of Technology Acceptance Model. *International Journal of Conceptions on Management and Social Sciences*. 4. p.1-4.
- TARHINI, A., ELYAS, T., AKOUR, M. A. & AL-SALTI, Z. (2016). Technology, Demographic Characteristics and E-Learning Acceptance: A Conceptual Model Based on Extended Technology Acceptance Model. *Higher Education Studies*. 6. p.72-89.
- TEH, P. S., ZHANG, N., TEOH, A. B. J. & CHEN, K. (2016). A survey on touch dynamics authentication in mobile devices. *Computers and Security*. 59. p.210-235.
- THIELSCH, M. T., ENGEL, R. & HIRSCHFELD, G. (2015). Expected usability is not a valid indicator of experienced usability. *Peer Journal Computer Science*. p.1-19.
- THIRUMOORTHY, D. K. (2015). Mobile computing. *International conference on interdisciplinary research in engineering and technology*. I. p.69-72.
- THOMAS, K. V., DR (2014). A diffusion theory perspective on the adoption of online shopping among youth in central Kerala. *International Journal of Innovative Research in Science, Engineering and Technology*. 3. p.16688-16694.
- TORNATZKY, L. G., FLEISCHER, M. & CHAKRABARTI, A. K. (1990). *Processes of Technological Innovation*. Lexington books.
- TORNATZKY, L. G. & KLEIN, K. J. (1982). Innovation characteristics and innovation adoption-implementation: A meta-analysis of findings. *IEEE Transactions on Engineering Management*. p.28-45.
- TSHABALALA, M., NDEYA-NDEREYA, C. & VAN DER MERWE, T. (2014). Implementing blended learning at a developing university: obstacles in the way. *The Electronic Journal of e-learning*. 12. p.101-110.
- UCT. (2017). *adfs/ls/* [Online]. Available: <https://vula.uct.ac.za/portal> [Accessed 30 May 2017]
- UD DIN, I., XUE, M. C., ABDULLAH, ALI, S., SHAH, T. & ILYAS, A. (2017). Role of information & communication technology (ICT) and e-governance in health sector of Pakistan: A case study of Peshawar. *Cogent Social Sciences*. 3. p.1308051.
- UFILING. (2017). *AboutUfiling* [Online]. Available: <https://www.ufiling.co.za/> [Accessed 30 May 2017]
- UJ. (2017). *ulink* [Online]. Available: <https://ulink.uj.ac.za/> [Accessed 30 May 2017]
- UKZN. (2017). *Login* [Online]. Available: <https://learn.ukzn.ac.za/> [Accessed 28 May 2017]
- UR, B., BEES, J., SEGRET, S. M., BAUER, L., CHRISTIN, N. & CRANOR, L. F. (2016). Do users' perceptions of password security match reality? CHI'16 May 07-12 2016. San Jose, CA,USA. ACM. p.1-13.

- VAITHYA, S., CHRISTY, A. & SARAVANAN, D. (2015). Two factor authentications for secured login in support of effective information presevation and network security. *ARPN Journal of Engineering and Applied Sciences*. 1. p.2053-2056.
- VANCOUVER, B. C. (2017). *Digital, Social and mobile in 2017: We are social compendium of global digital statistics* [Online]. We are social and HootSuite. [Accessed 11 June 2017]
- VENKATESH, V. & BALA, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*. 39. p.273-315.
- VENKATESH, V. & DAVIS, F. D. (2000). A theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*. 46. p.186-204.
- VENKATESH, V., MORRIS, M. G., DAVIS, G. B. & DAVIS, F. D. (2003). User acceptance of information technology: toward a unified view. *MIS Quarterly*. 27. p.425-478.
- VENKATESH, V., THONG, J. Y. & XU, X. (2016). Unified theory of acceptance and use of technology: a synthesis and the road ahead.
- VERKIJKA, S. F. & DE WET, L. (2016). e-Government development in Sub-Saharan Africa (SSA): Relationship with macro level indices and possible implications. IST-Africa Week Conference, 2016. IEEE. p.1-10.
- WANG, Q. (2014). Kernel principal component analysis and its applications in face recognition and active shape models. *Rensselaer Polytechnic institute*. 110 Eighth street, Troy, NY 1280 USA.
- WANG, Y.-S., LI, H.-T., LI, C.-R. & ZHANG, D.-Z. (2016). Factors affecting hotels' adoption of mobile reservation systems: A technology-organization-environment framework. *Tourism Management*. 53. p.163-172.
- WEI, W., LI, J., CAO, L., OU, Y. & CHEN, J. (2013). Effective detection of Sophisticated online banking fraud on extremely imbalanced data. *World Wide Web*. 16. p.449-475.
- WENG, W.-H. W. & LIN, W.-T. (2015). A mobile computing technology foresight study with scenario planning approach. *International Journal of Electronic Commerce Studies*. 6. p.223-232.
- WENTZEL, J. P., DIATHA, K. S. & YADAVALLI, V. S. S. (2013). An application of the extended technology acceptance model in understanding technology-enabled financial service adoption in South Africa. *Development Southern Africa*. 30. p.659-673.
- WIDYAWANI, N. L. & SANTOSA, P. I. (2017). Technology readiness and technology acceptance model in new technology implementation process in Low technology SMEs. *International Journal of Innovation, Management and Technology*. 8. p.113-117.
- WILLIAMS, M. D., RANA, N. P. & DWIVEDI, Y. K. (2015). The unified theory of acceptance and use of technology (UTAUT): A literature review. *Journal of Enterprise Information Management*. 28. p.443-488.

- WINGO, N. P., IVANKOVA, N. V. & MOSS, J. A. (2017). Faculty perceptions about teaching online: exploring the literature using the technology acceptance model as an organizing framework. *Online Learning*. 21. p.15-35.
- WITS. (2017). *Home* [Online]. Available: <https://cle.wits.ac.za/home/index> [Accessed 30 May 2017]
- YAO, F., YERIMA, S. Y., KANG, B. & SEZER, S. (2017). Continuous implicit authentication for mobile devices based on adaptive neuro-fuzzy inference system. IEEE International conference on cyber security, June 19-20 2017. London, UK. p.1-7.
- YASER, A., SLEWA-YOUNAN, S., SMITH, C. A., OLSON, R. E., GUAJARDO, M. G. U. & MOND, J. (2016). Beliefs and knowledge about post-traumatic stress disorder amongst resettled Afghan refugees in Australia. *International Journal of Mental Health Systems*. 10. p.1-9.
- YI-SHUN, W., HSIEN-TA, L., CI-RONG, L. & DING-ZHONG, Z. (2016). Factors affecting hotels' adoption of mobile reservation systems: a technology organization-environment framework. *Tourism management*. 53. p.163-172.
- YUNUS, M. (2014). Diffusion of innovation, customer attitudes and intention to use mobile banking. *Information and Knowledge Management*. 4. p.12-18.
- ZOGHEIB, B. & RABAA'I, A. (2015). University student perceptions of technology use in mathematics learning. *Journal of Information Technology Education: Research*. 14. p.417-438.

APPENDIX A: INTRODUCTION LETTER

Vaal University of Technology

10 August 2017

To whom it may concern

Introduction Letter: Magister Technologiae Research

The purpose of this research is to investigate users' perceptions on the security of mobile computing for adoption of e-applications in South Africa. This will cover the security mechanisms being used on mobile devices.

Students at Vaal University of Technology are requested to conduct a research study on a topic of their preference that will serve as part of their dissertation which they need to complete in order to graduate and receive their Magister Technologiae certificate. It is anticipated that the research report studies will be published in Vaal University of Technology internal journal for further study by other students who might need to carry on with their studies.

The purpose of this mobile computing questionnaire is to explain the users understanding, knowledge towards mobile computing security and assist on analyzing the results and be able to write the conclusion.

We would be grateful for any support that you may be willing to complete this mobile computing questionnaire, please bear in mind that any information received will be used for academic purpose. The questionnaire consists of 35 questions and which will acquire almost 15 to 20 minutes to complete. Demographic information and security mechanisms information will be asked if you choose to participate in this small survey. Furthermore with personal data which will be kept anonymous. These data will assist us to analyze the results based on demographic and other mobile computing security. Your support will be highly appreciated

If you should have any questions, please you are more than welcome to get in touch with me

Yours sincerely

Fhatuwani Vivian Mapande (vivica.mapande664@gmail.com)

APPENDIX B: QUESTIONNAIRE

Questionnaire: Users' perceptions on the security of mobile computing systems in South Africa.

Section A: Demographic Information

1. What is your gender?

☐ Male ☐ Female

2. What is your age?

☐ 18-25 ☐ 26-35 ☐ 36-45 ☐ Over 46

3. Which ethnic group best describe you?

☐ Asian ☐ Black ☐ White ☐ Indian ☐ Colored ☐ Other

4. What is your highest education level?

☐ High school ☐ Degree ☐ Postgraduate ☐ Other

5. What is your current occupation?

☐ Not working ☐ Working ☐ Pensioner ☐ Self-employed ☐ Other

Section B: Users' perceptions on the security of mobile computing

Please read each statement and then select your choice by clicking inside the square which best indicates how strongly you agree or disagree with the statement.

Strongly disagree=1; Disagree=2; Neutral =3; Agree=4; Strongly agree=5

Question 1-4: Perceived Usefulness of security mechanisms

- 1. I find using Password/PIN security mechanism on mobile computing useful to access e-applications**

| | | | | |
|--------------------------|--------------------------|----------------------------|--------------------------|--------------------------|
| Strongly Disagree | Disagree | Neither agree nor disagree | Agree | Strongly Agree |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

- 2. I find using fingerprint security mechanism on mobile computing useful to access e-applications**

| | | | | |
|--------------------------|--------------------------|----------------------------|--------------------------|--------------------------|
| Strongly Disagree | Disagree | Neither agree nor disagree | Agree | Strongly Agree |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

- 3. I find using combination of password and fingerprint security mechanism on mobile computing useful to access e-applications**

| | | | | |
|--------------------------|--------------------------|----------------------------|--------------------------|--------------------------|
| Strongly Disagree | Disagree | Neither agree nor disagree | Agree | Strongly Agree |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

- 4. I find using pattern security mechanism on mobile computing useful to access e-applications**

| | | | | |
|--------------------------|--------------------------|----------------------------|--------------------------|--------------------------|
| Strongly Disagree | Disagree | Neither agree nor disagree | Agree | Strongly Agree |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Question 5-8: Perceived Ease of use of security mechanisms

5. I find Password/PIN security mechanism easy to use on mobile computing to access e-applications

| | | | | |
|--------------------------|--------------------------|----------------------------|--------------------------|--------------------------|
| Strongly Disagree | Disagree | Neither agree nor disagree | Agree | Strongly Agree |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

6. I find fingerprint security mechanism easy to use on mobile computing to access e-applications

| | | | | |
|--------------------------|--------------------------|----------------------------|--------------------------|--------------------------|
| Strongly Disagree | Disagree | Neither agree nor disagree | Agree | Strongly Agree |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

7. I find using combination of password and fingerprint security mechanism easy to use on mobile computing to access e-applications

| | | | | |
|--------------------------|--------------------------|----------------------------|--------------------------|--------------------------|
| Strongly Disagree | Disagree | Neither agree nor disagree | Agree | Strongly Agree |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

8. I find using pattern security mechanism on mobile computing easy to use to access e-applications

| | | | | |
|--------------------------|--------------------------|----------------------------|--------------------------|--------------------------|
| Strongly Disagree | Disagree | Neither agree nor disagree | Agree | Strongly Agree |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Question 9-12: Aesthetic of security mechanisms interface

9. Security mechanisms interface is clearly structured and simple

| | | | | |
|--------------------------|--------------------------|----------------------------|--------------------------|--------------------------|
| Strongly Disagree | Disagree | Neither agree nor disagree | Agree | Strongly Agree |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

10. Security mechanisms' interface is beautiful

| | | | | |
|--------------------------|--------------------------|----------------------------|--------------------------|--------------------------|
| Strongly Disagree | Disagree | Neither agree nor disagree | Agree | Strongly Agree |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

11. The user interface for security mechanisms' input is designed for all levels of users

| | | | | |
|--------------------------|--------------------------|----------------------------|--------------------------|--------------------------|
| Strongly Disagree | Disagree | Neither agree nor disagree | Agree | Strongly Agree |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

12. Security mechanisms' interface is stylish

| | | | | |
|--------------------------|--------------------------|----------------------------|--------------------------|--------------------------|
| Strongly Disagree | Disagree | Neither agree nor disagree | Agree | Strongly Agree |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Question 13-16: Intention to adopt e-applications

13. I intend to use the e-applications frequently in my life

| | | | | |
|--------------------------|--------------------------|----------------------------|--------------------------|--------------------------|
| Strongly Disagree | Disagree | Neither agree nor disagree | Agree | Strongly Agree |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

14. I intend to use e-applications platform as soon as possible

| | | | | |
|--------------------------|--------------------------|----------------------------|--------------------------|--------------------------|
| Strongly Disagree | Disagree | Neither agree nor disagree | Agree | Strongly Agree |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

15. I plan to use the e-applications platform in the future

| | | | | |
|--------------------------|--------------------------|----------------------------|--------------------------|--------------------------|
| Strongly Disagree | Disagree | Neither agree nor disagree | Agree | Strongly Agree |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

16. I will recommend e-applications to others

| | | | | |
|--------------------------|--------------------------|----------------------------|--------------------------|--------------------------|
| Strongly Disagree | Disagree | Neither agree nor disagree | Agree | Strongly Agree |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Question 17-20: Relative Advantage of security mechanisms

17. PIN/Password security mechanism has more advantages which makes the security more efficient

Strongly Disagree Disagree Neither agree nor disagree Agree Strongly Agree

| | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|

18. Fingerprint security mechanism has more advantages which makes the security more efficient

Strongly Disagree Disagree Neither agree nor disagree Agree Strongly Agree

| | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|

19. Combination of PIN and fingerprint security mechanism has more advantages which makes the security more efficient

Strongly Disagree Disagree Neither agree nor disagree Agree Strongly Agree

| | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|

20. Pattern security mechanism has more advantages which makes the security more efficient

Strongly Disagree Disagree Neither agree nor disagree Agree Strongly Agree

| | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|

Question 21-23: Subjective norm on security mechanisms

21. Individuals who influence me think that I should use Password/PIN security mechanism on mobile computing to access e-applications

Strongly Disagree Disagree Neither agree nor disagree Agree Strongly Agree

| | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|

22. Individuals who influence me think that I should use fingerprint security mechanism on mobile computing to access e-applications

Strongly Disagree Disagree Neither agree nor disagree Agree Strongly Agree

| | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|

23. Individuals who influence me think that I should use pattern security mechanism on mobile computing to access e-applications

Strongly Disagree Disagree Neither agree nor disagree Agree Strongly Agree

| | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|

Question 24-26: Compatibility of security mechanisms

24. The function of PIN/Password security mechanism is compatible for e-applications on mobile device

Strongly Disagree Disagree Neither agree nor disagree Agree Strongly Agree

| | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|

25. The function of fingerprint security mechanism is compatible for e-applications on mobile device

Strongly Disagree Disagree Neither agree nor disagree Agree Strongly Agree

| | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|

26. The function of Pattern security mechanism is compatible for e-applications on mobile device

Strongly Disagree Disagree Neither agree nor disagree Agree Strongly Agree

| | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|

Question 27-30: Complexity of security mechanisms

27. Using PIN/Password security mechanism is less complex

Strongly Disagree Disagree Neither agree nor disagree Agree Strongly Agree

| | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|

28. Using Fingerprint security mechanism is less complex

Strongly Disagree Disagree Neither agree nor disagree Agree Strongly Agree

| | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|

29. Using Pattern security mechanisms is less complex

Strongly Disagree Disagree Neither agree nor disagree Agree Strongly Agree

| | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|

30. Using combination of password and fingerprint security mechanism is less complex

Strongly Disagree Disagree Neither agree nor disagree Agree Strongly Agree

| | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|