ACCEPTANCE OF BIOMETRIC AUTHENTICATION SECURITY TECHNOLOGY ON MOBILE DEVICES

By

W.R. Malatji

Student number: 214005720

Orcid.org/0000-0002-8970-1844

Thesis submitted in fulfilment of the requirements for the degree of

Master of Information and Communication Technology

In the Faculty of Applied and Computer Science

At the Vaal University of Technology

Supervisor: Prof Tranos Zuva

Co-supervisor: Dr Rene Van Eck

Vanderbijlpark Campus

Acknowledgements

I wish to thank:

- Prof Zuva and Dr. Rene Van Eck for their insightful and positive comments during the preparation and production of this study. Their ability to give so freely of their time has been greatly appreciated.
- M.J. Malatji for the support and provision of equipment in order for me to complete this study successfully.
- Miss C.J. Sehodi for her professional advice and valuable support.
- Finally, I would like to express my gratitude to my parents for their unwavering help and encouragement during my studies.

Declaration

I declare that this research project with the title: “Acceptance of biometric authentication security technology on mobile devices”, is my own work that has not been published anywhere else, except in parts, by anyone else unless I specifically state otherwise.

- Plagiarism, as I understand it, is when I present someone else's ideas and words as my own without properly acknowledging the source.
- Via a widely accepted style of quotations, references, and bibliography, I have completely recognised all terms, thoughts, and findings from other sources that I have used in this project.
- I am aware that plagiarism is considered a serious offence by the university and is subject to disciplinary action.

…… ……

Student signature Date

Dedications

I would like to dedicate this work to my mother, Mrs Maropeng Johanna Malatji, who provided all the necessary support and equipment for me to successfully complete this research. Moreover, I would like to thank my supervisors for their support and cooperation.

Abstract

Mobile devices are rapidly becoming a key computing platform, transforming how people access business and personal information. Accessing business and personal data using mobile devices requires authentication that is secure. The world is rapidly becoming connected and all users of mobile devices need to be clear regarding individual data security. As a result, biometrics for mobile devices has come into existence. Biometric technology can be applied on mobile devices to improve the trustworthiness of wireless services. Furthermore, it is of great importance and necessary to start paying attention to and investing in mobile biometric technologies, as they are quickly turning into tools of choice for productivity. In the literature review, it shows that few studies measured the acceptance of biometric authentication technology on mobile devices. This study seeks to find out the perceptions as to the acceptance of biometric authentication technology on mobile devices.

TAM2 was used as the foundation for generating the hypothesis and developing the conceptual framework for this study. This quantitative study used a survey-based questionnaire to collect data from 305 participants. The simple random sampling technique was used to select participants for this study. The response rate was 98% of the expected population, which was a total of 302 valid responses. A descriptive analysis was deployed to provide a description of respondents' demographic characteristics. SPSS was used to compute the multiple regressions in order to evaluate the research hypotheses.

The findings of this study revealed that perceived humanness, perceived interactivity, perceived social presence, perceived ease of use and subjective social norm, and perceived usefulness and trust are important determinants of customers' intention to accept and use mobile biometric devices. It was found that reliability is a good predictor of trust. On the other hand privacy, identity theft and combining data are also important determinants of trust. This work can be used to strengthen biometric authentication technology in-cooperation with mobile devices for simplicity of use. Since most mobile devices are used for personal and business information, further research on the acceptance of biometric authentication technology on mobile devices is needed.

Keywords: Technology acceptance, biometrics, mobile devices, mobile biometrics, intention to use.

List of publications

Malatji, W. R., Van Eck, R., & Zuva, T. (2020)-a. Acceptance of biometric authentication security technology on mobile devices. *2nd International Conference on Communication, Computing and Electronic System*, 733, 145-156.

Malatji, W. R., Van Eck, R., & Zuva, T. (2020)-b. Acceptance of biometric authentication security technology on mobile devices. *The 2nd International Multidisciplinary Information Technology and Engineering Conference.* Sol Plaatje University: Kimberly.

Malatji, W. R., Van Eck, R., & Zuva, T. (2020)-c. Understanding the usage, modifications, limitations and criticisms of Technology Acceptance Model (TAM). *Advanced in Science, Technology and Engineering Systems Journal*, 5 (6)**,** 113-117.

Table of contents

List of tables

List of figures

List of abbreviations and acronyms

ATT	Attitude
AUMBD	Actual Use of Mobile Biometric Device
BI	Behavioural Intentions
BU	Behaviour Use
DIT	Theory of Diffusion of Innovation
HMSAM	Hendonic-Motivation System Adoption
IS	Information Systems
IT	Information Technology
IU	Intention to Use
MBTAM	Mobile Biometric Technology Acceptance Model
MPT	Modern Portfolio Theory
PBC	Perceived Behavioural Control
PEOU	Perceived Ease of Use
PH	Perceived Humanness
PI	Perceived Interactivity
PP	Perceived Playfull
PSP	Perceived Social Presence
PU	Perceived Usefulness
SCT	Social Cognitive Theory
SMEs	Small Medium Enterprises
SN	Social Norm
SSN	Subjective Social Norm
TAM	Technology Acceptance Model
TIB	Theory of Interpersonal Behaviour
TPB	Theory of Planned Behaviour
TRA	Theory of Reasoned Action

UTAUT Unified Theory of Acceptance and Use of Technology

Chapter one: Introduction

1.1. Introduction

Mobile devices are increasingly being used not only for basic communications in a technological era but also as a tool to manage personal affairs and process data collected from anywhere at any time (Wang and Liu, 2009). In recent years, mobile device access to information has become commonplace in both business and personal settings. The world is becoming increasingly connected, and every mobile user needs to know that their data is secured (Kadena and Ruiz, 2018).

Safe authentication is required for access to business data from mobile devices, but traditional password schemes based on a mixture of alphanumeric and symbols are not popular and manageable, leading clients to avoid accessing business data on their devices entirely (Bao, Pierce, Whittaker and Zhai, 2011). More sensitive data is stored on these devices as their versatility expands, including e-commerce, entertainment, remote work, mobile banking, and internet access. Biometrics for mobiles was created as a result of these factors (Kadena and Ruiz, 2018).

For the protection of mobile devices and to improve the efficiency of wireless networks, it is preferable to use biometric technology (Clarke and Furnell, 2005). Any technique that accurately uses observable physiological or behavioural characteristics to differentiate one person from another is referred to as biometric technology (Kaur and Savedna, 2013).

Biometrics, which aims to identify an individual using distinct features of human physiological or behavioural characteristics, including voice, gait, signature, iris, face, and fingerprints, naturally provides a high degree of protection (Wang and Liu, 2009). Biometrics has traditionally relied on specialised instruments, such as infrared cameras for iris image acquisition, computer servers with large-scale capacity to perform recognition algorithms, and sensors of acceleration for gait acquisition, has several drawbacks, including operational difficulty, bulky size and costs that are extremely high (Wang and Liu, 2009).

This study focused on the acceptance of biometric authentication technology on mobile devices. It aimed to find out the perceptions as to the acceptance of biometric authentication technology on mobile devices. The study took place at the University of Technology.

1.2. Problem statement

In recent years, mobile device access to information has become commonplace in both business and personal settings. The world is becoming technically connected, and every mobile user needs to know that their data is secure (Kadena and Ruiz, 2018). Biometric technology is preferred to improve the security of mobile devices and the efficiency of wireless networks (Clarke and Furnell, 2005).

Many studies have been conducted on biometric devices and application adoption, consumer attitudes toward these devices, and performance effect measurements. That being said, only a few of the studies looked into the factors that have an influence on biometric device acceptance (James *et al*., 2017). Only a few studies were performed on the issues faced by users concerning biometric acceptance and use, according to Chau, Stephen, and Jamieson (2004), of the few studies that were undertaken to assess biometric technology acceptance.

There were just a few studies that focused on the acceptance of biometric authentication technology on mobile devices. Since mobile devices are used for both business and personal purposes, this study sought to determine the level of acceptance of biometric authentication technology on mobile devices.

1.3. Research questions

The main research question of this study was: What is the perception of acceptance of biometric authentication technology on mobile devices? This main research question was answered through the following sub-questions:

1.3.1. Sub-questions

- What has been done, according to the literature, to measure user acceptance of technology?
- What model can be proposed to measure the acceptance of biometric authentication technology on mobile devices?

- How does one measure the effect of every variable of the model in the acceptance of biometric authentication technology on mobile devices?

1.4. Aims and objectives of the study

The main aim of this study was to find out the perception of acceptance of biometric authentication technology on mobile devices. The aim was achieved through the following objectives:

- To study and determine what was done, according to the literature, to measure user acceptance of technology.
- To propose a model that could be used to measure the acceptance of biometric authentication technology on mobile devices.
- To measure the effect of every variable of the model in the acceptance of biometric authentication technology on mobile devices.

1.5. Methodology

Many studies have been undertaken on the adoption and acceptance of technology. This study was conducted using a quantitative research strategy. This method was chosen because previous related studies used it and it was proven to be suitable. The target population for this study was South African citizens in Johannesburg (Vanderbijlpark) only. The study chose only this population due to travelling restrictions under the world-wide pandemic COVID-19 and time restrictions.

This study used survey-based questionnaires that were categorised into two dissimilar sections to gather information from participants. The first section of the questionnaire aimed to collect background information which included questions associated with demographics, user experience of information technology, the use of internet and user experience of the internet scams. The second section of the questionnaire aimed to find out perceptions regarding the use of mobile biometrics.

1.6. Significance of the current study

Mobile devices are not only turning into productivity tools of choice but are also being used for personal, business and educational purposes. All persons who own mobile devices want to ensure the safety of their personal data. Recent devices are utilising biometric technology to authenticate users; however, this technology was tested on mobile devices with user acceptance by a small number of studies. This study aimed to find out the perceptions as to the acceptance of biometric authentication technology on mobile devices.

This study will contribute to the user acceptance of biometric authentication security technology on mobile devices not only in Johannesburg (Vanderbijlpark) but also in other provinces and cities both nationally and internationally. It is hoped that the research will increase the users' knowledge of the existing biometric authentication security technology on mobile devices and also enhance the users' willingness to use such devices. It has come to the researcher's attention that most technologies are not accepted and used because users are not aware of their existence. Therefore, it is hoped that this study will positively contribute to the users' awareness of the existing biometric authentication security technology on mobile devices.

The results of this survey will help decision-makers to be conscious of the issues that influence the users' decisions to admit and utilise a certain system so that they will be capable of taking them into consideration during the stage of the system development. It is hoped that future researchers will benefit from this survey as it provides a valuable information with regards to biometric authentication technology on mobile devices and there is a possibility for them to find answers for their research questions in this survey. Furthermore, this study can also be used to enhance the cooperation of biometric authentication technology on mobile devices.

1.7. Study contributions to knowledge

1.7.1. Contributions to theory

- The study contributed to the literature review on the issues of the acceptance of biometric authentication technology on mobile devices and to the body of knowledge in general.
- The study added value to the general understanding of the acceptance of biometric authentication security technology on mobile devices to research theory.

- The study contributed by providing a solution to the gap that was identified from the literature review.

1.7.2. Contributions to methodology

- The study determined the usefulness of deploying technologically advanced data by utilising online tools.
- The study contributed by providing the mathematical model that can be used to measure acceptance.

1.7.3. Technical contribution

- The study contributed to the awareness of the issues that affect' users' decisions to welcome and utilise a specific technology to decision-makers to consider during the development stage.

1.8. Ethical considerations

The participants were given the participant information sheet which informed them of the ethical considerations that the research observed. The form included the following ethics:

- Right to self-determination.
- Informed consent.
- The right to disclosure.
- Privacy and confidentiality.

All the above-mentioned ethics will be fully discussed later in chapter 3 of this study.

1.9. Scope and limitations of the current study

The scope of this study included South African citizens in Johannesburg (Vanderbijlpark), mobile devices, biometrics and User's perception of acceptance of biometric authentication technology on mobile devices. As with the majority of studies, the design of the current study

was subjected to two limitations which included lack of previous research studies on the topic and limited access to data.

1.10. Thesis outline

This section of the study provides a general review or summary of the complete thesis contents, which include this chapter as the first chapter. The section will start by presenting the chapter layout diagram for the current study.

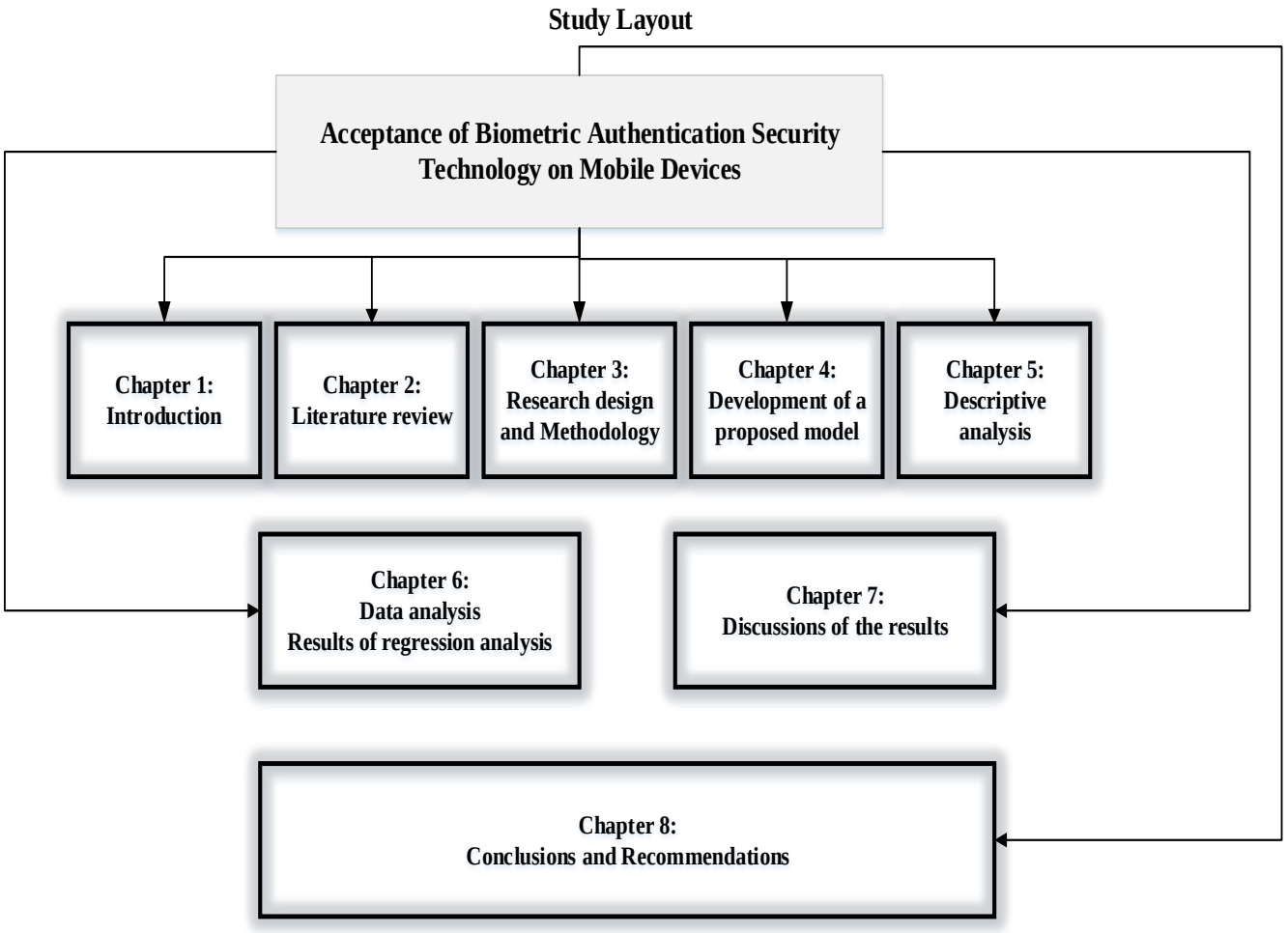


Figure 1. 1 Study layout for the current study

Chapter 2 continues the research by undertaking a literature review. Furthermore, it aims to advance the research by reviewing attempts previously made to answer the research questions. This chapter reviews the root of the research issues posed by the current study and continues to critically review the existing literature so that a clear current state of biometric acceptance on

mobile devices can be made. The chapter finally identifies the important issues related to mobile biometric acceptance.

Chapter 3 gives a general description of the methodology that was followed to investigate the research questions to find a possible solution for the research problem. This incorporates a detailed discussion of the philosophical background of the research method chosen. Moreover, this chapter describes the strategies used for data collection and the selection of research instruments and sampling.

Chapter 4 reviews the development of the proposed research model for the current study. Later, it provides a brief explanation of the theoretical model variables and hypotheses are presented.

Chapter 5 presents a descriptive analysis of the data obtained through data collection instruments. The questionnaire used in this quantitative study was carefully analysed to ensure that the data gathered was presented clearly with the aid of tables, percentages and charts, where possible.

Chapter 6 discusses the correlation association between independent and dependent variables that are incorporated in this study. Furthermore, this chapter demonstrates the outcomes of the hypothesis testing with regard to the acceptance of mobile biometric devices which were achieved by performing multiple regression analysis.

Chapter 7 analyses and discusses the obtained results from chapter 6. The hypotheses of the current study are tested by reviewing the determining factors of mobile biometric acceptance. Finally, all of the hypotheses will be presented in their numerical order.

Chapter 8 concludes the work of the current study by looking at the major research contributors. It then continues to provide a general description of the results and evaluates their practical theoretical implications. The limitations, including the suggestions for future research are also highlighted in this chapter.

Chapter two: Literature review

2.1. Introduction

In the field of research, technology acceptance has become a major concern. A number of models and frameworks have been developed to explain user acceptance of new technologies. This chapter continues the research by undertaking a literature review. Furthermore, it aims to advance the research by reviewing attempts previously made to answer all research questions. Since most mobile devices are used to store personal and business data, more research on the acceptance of biometric authentication technology on mobile devices is needed. Therefore, this chapter is arranged as follows; Acceptance of mobile devices, biometric acceptance, biometric user acceptance issues, mobile biometric authentication, implementation of biometrics on mobile devices, the benefits of mobile biometrics, the future of mobile biometric technologies, challenges and open issues of mobile biometrics.

2.2. Technology Acceptance Model (TAM) and theories

Researchers have been proposing frameworks or models to explore consumer acceptance of Information Technology and Information Systems in the research field. Acceptance is generally described as an opposition to the term 'denial' and refers to a positive choice to utilise advancement (Taherdoost, Sahibuddin and Jalaliyoon, 2012). According to Taherdoost *et al.* (2010), numerous researchers developed models and theories to explain and examine user acceptance and every single model determines various factors to describe user acknowledgment.

The question regarding user acknowledgment is linked to every researcher who wants to indicate which innovation will be most suitable for an organisation (Taherdoost and Sahibuddin, 2015). In addition, user acceptance is of great importance to the successful application of any modern innovation (Taherdoost and Sahibuddin, 2015). Moreover, it is of great importance to be aware that technology's characteristics play an important role in determining if persons taking part in an activity will utilise it or not (Taherdoost *et al.*, 2019).

Practitioners and academics are interested in identifying the factors that influence users' acceptance or rejection of modern technologies (Taherdoost and Masrom, 2009). Finding a response to this question will help them to refine techniques for analysing, anticipating, and

designing consumer responses to innovations (Dillion and Morris, 1996). Taherdoost, Sahibuddin and Jalaliyoon (2012) said that technology acceptance models and theories have been used to understand and predict user behaviour in a wide variety of domains such as dieting, education, voting, etc.

2.2.1. Technology Acceptance Model (TAM) background history

The importance of theories and models that predict and characterise information technology acceptance and use has grown in tandem with the growing popularity of customers' responses to IT (Taherdoost *et al.,* 2019). Researchers accepted and used theories and models like the theory of reasoned action (TRA), the theory of interpersonal behaviour (TIB), technology acceptance model (TAM) and social cognitive theory (SCT) to assess the use of emerging technology (Taherdoost *et al.,* 2019). Several studies have used original models to conduct research; however, the Technology Acceptance Model (TAM) is the primary focus of this paper.

The Technology Acceptance Model is one of the most influential extensions of Ajzen and Fishbein's (1980) theory of reasoned action (TRA) in the literature. TAM was formulated in the 1980s as a result of employees' failure to use information technology that had been made available to them (Davis, 1989). Its founders emphasised that the secret to increasing usage was to first increase acceptance of information technology, which could be assessed by asking people about their potential plans to use information technology (Holden and Karsh, 2009). Holden and Karsh (2009) indicated that recognising the factors that formed an individual's intentions can allow organisations to alter certain factors to boost acceptance and, as a result, increase IT use.

According to a previous TAM study, three variables are needed to define, predict, and manage acceptance (Fishbein and Ajzen, 1975). To arrive at this model, the founders used TRA, a universal social-psychological or behavioural theory that is useful in understanding various behaviours such as keeping fit, condom usage, and voting (Fishbein and Ajzen, 1975). As is customary when adapting theory to new situations, an initial study was conducted to determine what variables should be used in understanding IT use behaviour (Ajzen and Fishbein, 1980). Table 2.1 lists the variables that were used to construct the first TAM model.

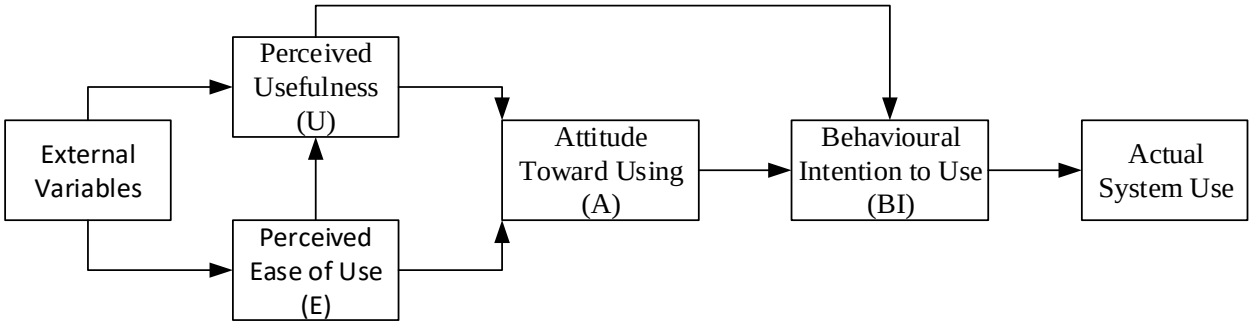


Figure 2. 1 Technology Acceptance Model (TAM) (Source: Davis, Bagozzi and Warshaw, 1989)

TAM, according to Bagozzi, Davis and Warshaw (1992) replace many of the TRA's attitude steps with several technology acceptance behaviours, such as ease of use and usefulness. Furthermore, TAM and TRA, which both have strong behavioural components, assume that once a person develops a willingness to act he or she can act freely and without restriction. (Legris, Ingham and Collerette, 2003) propose that TAM be expanded to include variables responsible for modifying processes, which can be accomplished by incorporating the innovation model into TAM.

2.2.2. Usage and modifications of TAM

TAM has been used by a number of researchers to conduct their studies. It was used by Sanchez-Franco (2010) to examine the learning efficacy of using technology as a podium for learning. The outcomes of the research emphasised that Perceived Ease of Use (PEOU), Perceived Usefulness (PU), and perceived playfulness may all be used to accurately predict a student's learning behaviour purpose. Kim (2010) used the theory of planned behaviour and the expectation-confirmation model for 207 mobile data service clients to find out their behavioural intention to continue utilising the service. The study's results revealed that customer acceptance, PU, and perceived playfulness were the most important factors in customers continuing to use the service.

Kim (2010) used TAM to investigate Chinese consumers' behavioural intention of the instant messenger. The decision has been made that PU and PP significantly affected consumers' attitudes. Using the theory of planned behaviour, it was discovered that SN and perceived behavioural control may well have a significant effect on Behavioural Intention (BI).

Furthermore, Davis, Bagozzi, and Warshaw (1989) researched the use of email and file processing applications by one hundred and twenty IBM Canadaian Laboratory employees. They discovered that workers' PU, PEOU, and software use were found to be strongly and significantly associated.

Ramos, Ferreira, Freitas and Rodrigues (2018) used TAM to measure the effect of trust on the intention to use mobile banking. The results of their study revealed that security (as perceived security) has a direct and positive effect on trust, privacy (as perceived privacy) has a direct and positive effect on trust and trust has a direct and positive influence on the intention to use. Moreover Shanab and Talafha (2015) used TAM to measure the internet banking adoption and found that reliability (as perceived reliability) has a positive influence on trust.

Tuner *et al.* (2010) used TAM to determine whether the model can predict the actual use of a system. The findings of their study revealed that IU is an important determinant of actual usage of seventy-one appropriate studies. Horton, Buck, Waterson and Clegg (2013) found that the greater the intention to use, the greater the actual use of the intranet.

Stock and Merkle (2018) used TAM in their study of a comparison of innovation behaviour cues. In their study, they maintained that consumer's acceptance of robots will depend not only on their perceived functionality but will also depend on social-emotional elements which include; perceived humanness, perceived interactivity and perceived social presence. Each of these three elements was found to be the determinant of consumer's willingness to accept service robots.

TAM was used by Liao *et al.* (2018) to investigate the behavioural purpose (BI) of students in higher education institutions and to evaluate their specialised capacity in e-book development using a web-based application assessment system. The findings revealed that participants' machine self-efficacy has a positive impact on PU and PU and PEOU. The PU and PEOU of participants had a significant and direct impact on their decision to use the system. As a result, when a person has higher machine self-efficacy and a higher opinion of the utility and ease of use of the web-based valuation framework, that person is more likely to use it.

TAM theory has undergone several revisions. TAM2, for example, removed the attitude (ATT) variable from the model, which had previously arbitrated some of the effects of perceived usefulness (PU) and perceived ease of use (PEOU). TAM2 also provided a subjective norm

variable to capture the social impact that drives end-users to favourably evaluate and welcome information technology (SN) (Venkatesh, Morris, Davis and Davis, 2003). The connections amongst the variables that were hypothesised from the theory that suggest and motivate the combination of TAM and DIT are:

- Social influence does not influence the complexity of understanding.
- Social influence directly influences triability.

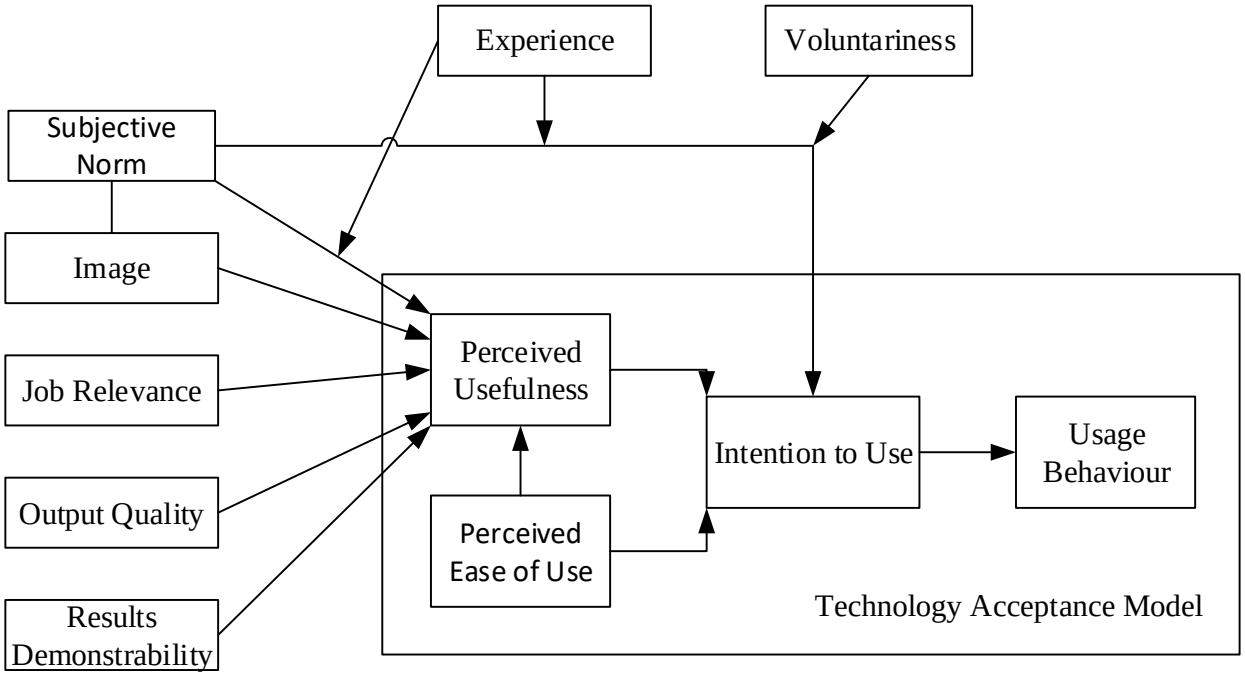


Figure 2. 2 TAM 2 (Source: Venkatesh and Davis, 2000)

Recently, an impressive effort to bring together the information technology acceptance writings resulted in the creation of a unified theory of acceptance and use of technology (UTAUT), a theory with clear similarity to TAM (Venkatesh, Morris, Davis and Davis, 2003). Unified Theory of Acceptance and Use of Technology includes putting perceived usefulness into a performance expectancy construct, perceived ease of use into effort expectancy, and subjective norm into social influence. Modern to the UTAUT, but not to the information technology acceptance study is commonly the use of easing circumstances as a determinant of behavioural intention (Taylor and Todd, 1995). UTAUT is a modern but capable theory. Prior experiments of ATAUT described a magnificent 70 percent of the behavioural intention variance and at most 50

percent in actual use (Taylor and Todd, 1995). Unified Theory of Acceptance and Use of Technology (UTAUT) has been embraced by current studies in health care. These include:

- MPT stands for Modern Portfolio Theory. As part of a national science foundation-funded dissertation thesis, Scherer (2005) designed the technology model and corresponding human being independent of TAM. Scherer's (2005) text explains current portfolio theory in detail.
- HMSAM (Hedonic-Motivation System Adoption Model): TAM has been influential in explaining the use of multiple systems (i.e., E-Learning, web portals, learning management system, etc.) (Fathema and Sutton, 2014; Fathema, Shannon and Ross, 2015). TAM, on the other hand, is not ideally suited to describing the implementation of entirely innate or hedonic structures (e.g. learning for pleasure, music, online games, etc.). HMSAM was built to better the understanding of the Hedonic-Motivation System Adoption Model (Lowry *et al.*, 2013).
- Extended TAM: Some studies have proposed that the original TAM be expanded by adding external variables to explore the effects of external influences on consumer attitude, actual usage, and behavioural intention of an invention (Fathema and Sutton, 2014; Fathema, Shannon and Ross, 2015). This model was adopted as a means of gaining support for health-care advancements (Nadri *et al.*, 2018).

Wu (2011) indicated that the Technology Acceptance Model and its enhanced variants are not suitable for all applications because they leave out key constructs like perceived risk. Thus, TAM has proven to be a widely accepted model that can be extended and modified (Wu, 2011 and Lopez-Nicolas, Molina-Castillo and Bouwmam, 2008).

Since the TAM theory has undergone multiple changes, the table below lists and describes the variables in TAM and related models.

Table 2. 1 TAM variables and related models

Variable	Definition	Models that contain the variable
Behaviour Use (BU)	One specific behaviour of interest shown by persons who pay close attention to a precise information system	TRA/TPB, TAM, TAM2, UTAUT
Behavioural Intention (BI)	A person's motivation or desire to put an effort to carry out the desired behaviour	TRA/TPB, TAM2, TAM, UTAUT
Attitude (ATT)	A person's subjective assessment of objective behaviour on a specific dimension	TAM, TRA/TPB
Perceived Ease of Use (PEOU)	A person's perception that using an IT framework would be easy	TAM, TAM2
Perceived Usefulness (PU)	A person's perception that using an IT framework will better work results	TAM, TAM2
Subjective Norm (SN)	A person's perception of the degree to which relevant individuals favour or are against the objective behaviour	TAM2, TRA/TPB
Perceived Behavioural Control (PBC)	A person's perception of how easy or difficult it will be to make the objective behaviour of elements that hinder or enable the behaviour, or of the degree of control that an individual has over performing the behaviour	TPB
Effort Expectancy	(Refer PEOU)	UTAUT
Performance Expectancy	(Refer PU)	UTAUT
Social Influence	(Refer SN)	UTAUT
Facilitating Conditions	(Refer PBC)	UTAUT
Behavioural Beliefs, Normative Beliefs and Control Beliefs	A person's perspective on specific positive or negative outcomes of implementing objective behaviour.	TRA/TPB

(Source: Wu, 2011 and Lopez-Nicolas, Molina-Castillo and Bouwmam, 2008)

2.2.3. Summary of TAM and modifications

The Technology Acceptance Model (TAM) has been revised, and the table below summarises the TAM and modified versions, as well as their goals.

Table 2. 2 Summary of TAM and modified versions

TAM and modified versions	Model Aim	Source
TAM	TAM was developed to better understand the natural chain that connects external variables to user acceptance and natural usage in a company. TAM aids in understanding the context of perceived ease of use.	Venkatesh and Davis (1989)
TAM2	TAM2 aims to understand perceived utility in order to develop workplace engagements that will improve user adoption of a new system.	Venkatesh, Morris, Davis and Davis (2003)
UTAUT	The unified theory of acceptance and use of the technology model shapes a unified model as a suitable instrument for managers required to measure the probability of modern technology introduction success.	Venkatesh, Morris, Davis and Davis (2003)
TAM3	TAM3 provides a combined model with significance allocated based on perceived utility and perceived ease of use, allowing managers and decision-makers to make informed decisions about interventions.	Venkatesh and Bala (2008)

2.2.4. TAM criticisms and limitations

Numerous scholars have cited the Technology Acceptance Model (TAM) because of its simplicity, without taking into account its actual use in their studies. Some of the TAM criticisms and shortcomings are discussed in this section, based on the use of model technology-related researches in various disciplines.

2.2.4.1. TAM criticisms

TAM has been widely criticised, irrespective of how often it is being used, resulting in the founders having to try to re-explain it frequently. TAM criticisms as a "theory" include its dubious heuristic value, limited explanatory and foretelling capacity, the triviality of critique, and lack of practical utility (Benbasat and Barki, 2007). TAM, according to Benbasat and Barki (2007), shifted researchers' focus away from other important research topics, creating the illusion of advancement in information accumulation. Furthermore, different researchers have attempted to expand TAM on their own for it to adjust to continually evolving IT conditions, resulting in a state of theoretical chaos and uncertainty (Benbasat and Barki, 2007).

Generally, TAM is based on a person's use of a computer, with an abstract idea of Perceived Usefulness (PU) and disregard for the essential social methods of Information Systems (IS) development and application, with no question as to "where many technologies are best and social after-effects of using Information Systems (IS)" (Benbasat and Barki, 2007). Lunceford (2009) maintains that the system of PU and PEOU is not capable of noticing other issues, for example, cost and structural imperatives that motivate users to adopt an invention.

Legris, Ingham and Collerette (2003) claim that TAM and TAM2 are responsible for no more than 40% of a technical framework's usage. Li (2020) went through the limitations of TAM implementation in an organisation setting in depth, indicating that even with a simple, easily applicable model, better predictive capability can be achieved when exact first screening methods are implemented.

The studies conducted by Hu, Chau and Sheng (1999); Wu and Wang (2005) and Pikkarainen, Pikkarainen and Karjaluoto (2004) found that PEOU is unlikely to be a contributing factor of attitude (ATT) and intention to use. Li (2020) also reported the same outcomes when

undertaking a study on the adoption of Blockchain technology. A study undertook by Okafor, Nico and Azman (2016) found that Perceived Ease of Use (PEOU) does not influence the adoption of multimedia online innovations for Malaysian SMEs. Similar outcomes were outlined by Hong Kong when evaluating SMEs (Li, 2020).

2.2.4.2. TAM limitations

To apply a theoretical structure, several factors must be taken into account, and researchers must be aware of the various limitations that exist. Maruping, Bala, Venkatesh and Brown (2016) said that to better understand the factors that promote improved use of information technology, it is essential to have a strong theoretical and implementation knowledge of systems and models by which information technology use is analysed.

Some of the limitations of the Technology Acceptance Model relate to the variable that refers to the behaviour of consumers, which is necessarily evaluated over subjective measures (for example, BI and social influence) (Maruping, Bala, Venkatesh and Brown, 2016). Nonetheless, social influence as SN refers to when someone is influenced by "word of mouth" from one of his or her co-workers (Maruping, Bala, Venkatesh and Brown, 2016).

The second limitation of TAM is that emphasis of behaviour fails to be quantified dependably in observed research, owing to numerous subjective factors, for example, the values and norms of societies and personal characteristics and personality attributes (Ang, Ramayah and Amin, 2015; Shan and King, 2015). As a result, a relative or friend's claim that might influence technology usage by strict social pressure is a highly falsifiable attribute (Ang, Ramayah and Amin, 2015; Shan and King, 2015). Even if it might be correct in theory or for individual utilisation of innovation, the conceptualisation might not be credible or precise in a workspace.

2.3. Acceptance of mobile devices

Any device that can be easily carried or link to a network, such as the internet, is referred to as a mobile device (Lindsay, Sultany & Reader, 2010). Characteristics of the aforementioned mobile devices are their small size (small enough to be handheld), they are lightweight (they weigh less than a kilogram) and have a display screen with touch input or a small keyboard (Kljunic and Vukovac, 2015). Mobile devices are now equipped with high-performance hardware such as quad-core CPU (Central Processing Unit), high-performance GPU (Graphics Processing Unit), high-speed flash storage, etc. Moreover, the costs of these devices are now affordable for average users (Reddy, Rattani and Derakhshani, 2016).

Less research on biometric mobile devices was performed, and the benefits and drawbacks of such devices were addressed (Vrana, 2018). While fewer studies have been conducted on the positive and negative aspects of those developments, it is, according to Vrana (2018), still unclear what factors influence the use of biometric authentication technologies on mobile devices in education, workplace, government, etc. and whether or not this usage has a long-term impact on overall growth and personal achievement. Specialised hypotheses are used to understand the process of technology adoption in this case.

Earlier research on mobile technologies has revealed significant relationships between perceived usefulness (PU) and behavioural intention (BI), and perceived ease of use (PE) and behavioural intention (BI) (Parveen and Sulaiman, 2008). However, Ursavas (2015) concluded an insignificant relationship between perceived ease of use (PE) and behavioural intention (BI). In addition, research on e-learning found contradicting results for perceived ease of use (PE) and behavioural intention (BI) relationship as some studies found it significant while others concluded it to be non-significant (Lee, Park, Kang and Park, 2009).

Other studies have also assessed the influence of TAM primary constructs on mobile phone usage and these studies found that PE was significantly related to BI and the relationship between PU and BI was also significant (Van Biljon and Kotze, 2008). It was also observed that TAM research on mobile phones is still lacking, especially on the instructors' perceptions and this emphasises the need to conduct further research on these variables (Mohamed, Shaari, Ismail

and Anuar, 2018). Based on the above notion, the study conducted by Mohamed, Shaari, Ismail and Anuar (2018) hypothesises:

- There is a significant relationship between perceived usefulness (PU) and behavioural intention (BI) of using a mobile technology device.
- There is a significant relationship between perceived ease of use (PE) and behavioural intention (BI) of using mobile technology device.

TAM studies have also extended the model by incorporating the external variable of prior mobile technology experience (ME) to the main variables of PE and PU (Mohamed, Shaari, Ismail and Anuar, 2018). Analysis on the relationship between ME and PE exhibited inconclusive results because Theng, Sharma and Tan (2009) found a significant relationship but other research concluded with an insignificant finding. Similar contrasting results were also found in the relationship between ME and PU as Tan, Ooi, and Phusavat (2012) concluded a significant relationship, whereas Mac Callum, Jeffrey and Kinshuk (2014) discovered an insignificant relationship.

As such, Mohamed, Shaari, Ismail and Anuar's study (2018) was performed to further explore the relationships between ME and PE and ME and PU in order to provide a better comprehension and offer additional experimental confirmation, specifically in the context of mobile technology device acceptance. Following this, their study hypothesises:

- There is a significant relationship between prior mobile technology experience (ME) and perceived usefulness (PU) of mobile technology devices.
- There is a significant relationship between prior mobile technology experience (ME) and perceived ease of use (PE) of mobile technology devices.

Since external variable ME has been included in the model, the independent variables of PU and PE functioned as mediating variables toward the dependent variable of BI (Mohamed, Shaari, Ismail and Anuar, 2018). Previous studies have found that PU mediated the relationship between prior experience and BI of using smartphones among Korean students and employees' experience with usage behaviour of word processor applications and e-mail (Burton-Jones, and Hubona, 2006).

Even though the variable PE had an insignificant mediating effect on BI, it was found that experience had a direct effect on system usage (Burton-Jones, and Hubona, 2006). The reason for this finding is that the users would have probably applied the technology since it had already become a habit for them to use it without taking into account the ease of using it (Burton-Jones, and Hubona, 2006). The above arguments have led Mohamed, Shaari, Ismail and Anuar‘s study (2018) to hypothesise:

- Perceived usefulness (PU) mediates the relationship between prior mobile technology experience (ME) and behavioural intention (BI) of using mobile technology.
- Perceived ease of use (PE) mediates the relationship between prior mobile technology experience (ME) and behavioural intention (BI) of using mobile technology.

2.4. Biometric acceptance

Biometrics originate from the Greek words' bio (which means life) and metrics (which means to measure) (Bhargava and Ochawar, 2013). The term "biometrics" refers to the application of current statistical methods to the calculation of biological objects. A biometric system is, at its heart, a pattern recognition system. It can link a specific set of physiological or behavioural characteristics to those retrieved from a person previously, and classify the latter (Jain, Ross and Prabhakar, 2004).

There have been many studies that were undertaken to determine the technical matters associated with biometric frameworks, for example, the accuracy and performance of various algorithms as well as biometric extraction methods (Kong, Zhang and Li, 2003 and Gutkowski, 2004). The international biometric foundation founder notes that fewer studies were undertaken on the user psychological matters and human factors that are related to biometric usage (Ashbourn, 2004, p. 9).

With the exception of Deane, Barelle, Henderson and Mahar (1995); Furnell, Dowland, Illingworth and Reynolds (2000); Clarke Furnell, Rodwell, Reynolds (2002); Giesing (2003) and Ho, Stephens and Jamieson (2003), many of the studies that were undertaken in this field have evaluated only technical aspects of biometrics.

Of the few researches that investigated biometric technology acceptance, it was only Ho, Stephens and Jamieson (2003) and Giesing (2003) who carried out empirical investigations on the issues related to biometric acceptance and usage. Earlier papers, Deane, Barelle, Henderson and Mahar (1995); Furnell, Dowland, Illingworth and Reynolds (2000), and Clarke Furnell, Rodwell, Reynolds (2002) - all surveyed the acceptability of various biometric methods, but the reasons behind such acceptability were not taken into consideration. Superficial decisions were taken based upon conjecture but not as a consequence of an empirical survey.

Deane, Barelle, Henderson and Mahar (1995) undertook a survey to compare behavioural acceptance and psychological biometric methods. The findings of the study revealed that biometric methods, in general, have a low rate of acceptability except for voice, fingerprint and hand-geometry. Moreover, signature analysis, retina scanning, pointing (mouse) and keystroke had the lowest rate of acceptability.

Furnell, Dowland, Illingworth and Reynolds (2000) as well undertook a similar survey to evaluate the attitudes of the public to alternative forms of client verification in comparison with passwords. The findings of the study revealed that face, keystroke, signature, fingerprint, iris, mouse dynamic including voice had a high level of client acceptability

Newspoll (2012) surveyed 1206 respondents aged 18 years and more to discover the level of the acknowledgment of biometric innovation (facial recognition in particular) from the Australian public. This was accomplished by asking how worthy they thought it was if this innovation was to be utilised in specific circumstances. The findings revealed that 95% of respondents were in support of the security if it was to be utilised by staff at the airport as a means of passenger identification on police watch-lists.

The same study was conducted by Unisys (2012) and it was found that 92% of respondents supported that the security can be used by the police to identify individuals from the video footage that is obtained from security cameras. However, more than a quarter of the respondents considered this security to be an unacceptable technology to use. Other respondents were concerned about the use of this security by the social media companies (for example, Facebook). It was discovered that 50% of the respondents said this technology was unacceptable to be used (Unisys, 2012).

Clarke Furnell, Rodwell, Reynolds (2002) undertook a survey on recent mobile subscribers regarding the security of their cell phones. The study presented various biometric authentication methods to participants as alternative authentication measures to secure their cell phones. The findings of the study revealed that all of the presented biometric authentication methods were favoured.

However, the limitation of the research conducted by Deane, Barelle, Henderson and Mahar (1995), Furnell, Dowland, Illingworth and Reynolds (2000) and Clarke Furnell, Rodwell, Reynolds (2002) was that there was no attempt was made to find out the level of experience that the participants had on biometrics. Participants might have responded based on the actual use or on the little knowledge they had about the biometric method, but the analysis was not carried out to determine whether the experience about biometrics can have an effect on user perception or not. Moreover, the studies only focused on the comparison of the acceptability of various biometric methods. The undertaken survey did not attempt to find out some reasons why one biometric method was preferred/accepted more than others. Lastly, the survey did not try to find out the reasons for and determining factors of biometric acceptance. Decisions were taken based on conjecture and speculation rather than experiential evidence.

However, Giesing (2003), found out some of the factors that had an influence on biometric acceptance and arrived at a conclusion that social factors and user perception were issues behind biometric technology adoption. The outcomes of this study brought about the development and/ or creation of the technology adoption model derived from TAM created by Davis (1989).

Nevertheless, the overall issues that were identified by Giesing's (2003) were also discovered by Ho, Stephens and Jamieson's (2003) study within their Biometric Acceptance Model that was derived from TAM by Venkatesh and Davis (2000). The dissimilarities between these two models are that Ho, Stephens and Jamieson (2003) incorporate the inhibiting and driving external forces that are behind the client and social factors discovered by Giesing (2003). For this reason, the current study examined the biometric user acceptance model by Ho, Stephens and Jamieson (2003) in more detail.

The survey undertook by Ho, Stephens and Jamieson (2003) investigated issues associated with the acceptance of biometric authentication security technology by interviewing and distributing surveys to managers and biometric authentication system users. Through this, Ho, Stephens and Jamieson (2003) discovered inhibitors and drivers which resulted in the development of the biometric user acceptance model.

In measuring variables of their model, the following was found:

- **Perceived usefulness**

In the context of biometrics, Ho, Stephens and Jamieson (2003) redefined perceived usefulness as "the degree to which a person believes that using a particular biometric system would fulfil the organisation's security access requirements in a particular domain". Job performance as well as result demonstrability were removed as determining factors of biometric acceptance since they are not in any way directly associated with biometric authentication systems. Ho, Stephens and Jamieson (2003) maintain that result demonstrability is irrelevant to biometrics because it is a "preventive innovation". Moreover, the advantages of biometric authentication technology are tangible.

Ho, Stephens and Jamieson (2003) enhanced TAM2 to incorporate reliability, security and identity assurance as determining factors of perceived usefulness of a biometric system. Ho, Stephens and Jamieson (2003)'s findings revealed that subjective norm, security, information sensitivity and identity assurance were important determinants of perceived usefulness and identity assurance and were the reasons biometrics was adopted. Reliability and security ranked high in their significance; nevertheless, interestingly, reliability and security were not major concerns to clients and managers as they assumed that the biometric system employed in their organisation was reliable.

Moving from TAM2, the influence of subjective norm will appear only in a non-voluntarily or mandatory system usage scenery where a referent has the strength to prize or punish non-behaviour (Venkatesh and Davis, 2000). Biometric authentication technologies are mostly subject to a kind of mandatory usage, and one might maintain the TAM relevance in such circumstances, though an environment that is mandated might still result in clients having a negative attitude towards the system.

Brown, Massey, Montoya-Weiss and Burkman (2002) argued that if usefulness perceptions are less, negative attitudes can increase which may lead to negative repercussions. This might result in sabotage or clients abusing the system, for example, granting Tailgaters access into the building and therefore bypassing the verification system. Thus, it is of the most importance to have a clear understanding of clients' perceptions in order to educate and take to the next level a positive attitude towards technology as well as its usage.

- **Perceived ease of use**

Ho, Stephens and Jamieson (2003) left the description of perceived ease of use untouched as the original description, "the degree to which a person believes that using a particular system would be free of effort" (Davis, 1989) is applicable to the biometrics domain. Ho, Stephens and Jamieson (2003) also added perceived safety, accuracy, hygiene, visibility, perceived invasiveness as well as perceived safety as determining factors of perceived ease of use.

The findings of this study revealed that perceived safety, convenience as well as hygiene were the most important factors that determine perceived ease of use. Convenience was found to be an important factor of acceptance with the majority of users providing types of conveniences as reasons why they preferred the system. Nonetheless, the survey also indicated that security comes before convenience, as the advantage of easing the security process if it is comprised was not found (Ho, Stephens and Jamieson, 2003).

Perceived safety indicates beliefs that individuals have concerning safety that might not be true, for instance, iris scanners are only capturing pictures of an individual's eye yet clients might be worried about damage to their eyes. Hygiene was a leading factor that determines acceptance for those clients who need to interact with the biometric system directly, for example, fingerprint scanning. Clients who utilise iris-based systems do not need to directly interact with the system, hence there are no hygiene issues (Ho, Stephens and Jamieson, 2003).

- **Intention to use**

Ho, Stephens and Jamieson (2003) added privacy as a determining factor of intention to use. Their study concerning privacy issues found that the concerns associated with privacy incorporate identity theft, combining data and function creep. However, they discovered that privacy was not that much of a concern as, "users seemed to place considerable trust in the

organisation, where simple assurance regarding the privacy of their biometric data seemed to appease them".

2.4.1. Biometric user acceptance issues

In terms of utilising biometrics for the aim of identification and authentication, Jain, Ross and Prabhakar (2004) discovered the following issues that require consideration in the biometric technology adoption:

- Performance: refers to the verification speed and accuracy and required resources to accomplish the desired verification speed and accuracy, including the environmental and operational factors that have an effect on the speed and accuracy.
- Acceptability: Denotes the degree to which individuals are intending to welcome the utilisation as a specific biometric identifier in their everyday life
- Circumvention: Reflects the ease of fraudulent behaviour to which the system can be exposed.

More issues associated with user acceptance were discovered in a qualitative survey undertaken by Ho, Stephens and Jamieson (2003). These included:

- Security: security incorporates the availability of information used, integrity, confidentiality and integrity.
- Visibility: the direct interaction level that is needed during system utilisation.
- Perceived invasiveness: apparent extent an individual's self is imposed upon.
- Privacy invasiveness: the disturbance to an individual's ability to have control over personal information.
- Perceived safety: beliefs of an individual concerning the influences that the system might have on his or her well-being or health.
- Information sensitivity: perceived sensitivity of job materials being secured by the biometric system.
- Identity assurance: assurance that only individuals who are authorised are given access.
- Reliability: the probability that the system maintains its success (not failure) in accomplishing ease of use of the system.

- Convenience: it is a reduction of effort through utilising the system and thereby improving ease of use of the system.

A study that was undertaken by Giesing (2020) also discovered issues that have an influence on user perception related to biometric use; however, the study was limited by the context of electronic business. Giesing (2020) discovered social factors as well as privacy, fraud and trust as influential factors of biometric adoption.

The table below shows the most popular biometric technologies as well as the degree of user acceptability for each form.

Table 2. 3 Common biometric technologies

Characteristic	**Method**	**Performance factor**	**User acceptance**	**Acquisition Device**
Fingerprints	Patterns of fingerprints are captured and compared	Dryness, dirt, worn, aged fingerprints.	Medium	Desktop peripheral, PCMCIA card, mouse, chip or reader embedded in the keyboard
Face	Facial features are captured and compared	Lighting, age, glasses, hair, environment	Medium	Video camera, PC, single-image camera
Retina	Patterns of blood vessels on the retina are captured and compared	Glasses, difficult to use	Low	Proprietary desktop or wall-mountable unit
Iris	Patterns of iris are captured and compared	Poor lighting, movement	High	Infrared-enabled video camera, PC camera
Voice	Cadence, pitch, and tone of the vocal tract are captured and compared	Noise, colds, weather, age, equipment, environment	High	Microphone, telephone
Hand geometry	Dimensions of hand and fingers are measured and compared	Hand injury, age, jewellery	High	Proprietary wall-mounted unit

Signature dynamics	Rhythm, acceleration and pressure flow of signature are captured and compared	Changing or erratic signatures	High	Signature tablet, motion-sensitive stylus

(Source: Allan, 2003 and Harris and Yen, 2002)

2.4.2. Biometric identification system: advantages and disadvantages

Biometrics have both benefits and drawbacks. User perception associated with security (resistance to track, reliability and accuracy), costs (expenses), and intrusiveness, template storage (capacity planning and location) and free of effort (ease of use) when choosing a particular biometric verification method must be taken into consideration by organisations (Allan, 2003). Tables 2.4 and Table 2.5 provide a summary of the benefits and drawbacks of biometric authentication systems, according to Allan (2003) and Harris and Yen (2002).

Table 2. 4 Summary of biometric advantages

Advantage	**Why?**	**Improvements**
PINs absent	Lower support costs	Efficiency
Users are known	Information remains confidential	Decision making
Unable to be shared	Upheld integrity of information	Reliability
Template usage	Fails biometric recreation	Security
Security increased	Information regarding biometrics will not get lost	Security
Convenience increased	Information regarding biometrics is always available	User acceptance
Lower costs	Removal of password management overheads	Economical
Security levels	Modify to business needs	Customizability

(Source: Allan, 2003 and Harris and Yen, 2002)

Albrecht (2003) highlighted that biometrics can deliver:

- Conventional security: In the authentication system, biometric techniques are responsible for the provision of improved security. A verification system that is based on the possession principle and knowledge usually requires authorization using a token along

with a PIN (e.g. smart card). The drawbacks of these traditional identification methods are that they can easily be forgotten or lost, the code or card may be stolen and their transferability (whether forced or voluntary) means they lack distinctive personal verification. The security of a knowledge-based method primarily depends on the individuals keeping their codes a secret.

- Unforgettable: The features of a biometric are unforgettable.
- Secure from theft: Features of biometric cannot be stolen, under normal circumstances
- Transferable – Biometric features are un-transferable.

Table 2. 5 Summary of biometric disadvantages

Disadvantages	**Why?**	**Decreases**	**Alternatives**
Publicity of biometric	Access to others	Security	Protection of biometric
Scans that are faulty	Enough authentication time	Efficiency	Enhance process
Inconvenience	Upset users	Productivity	Utilise alternative biometric
Cost	Deter business from using	Security	Show gain from systems
Education	Time is needed for this	Productivity	Whitepaper availability
People's views	Must overcome issues	Productivity	Implementation after address
Default threshold	Others might be beaten	Security	Increase threshold
Privacy issue	Data misuse	Client acceptance	Protection of information
individual religious and cultural issues	Hygiene and Connotation of criminal	Client acceptance	alternative biometric utilisation
Overall user sustainability	Body part missing	Client acceptance	Utilise a "fall-back" system

(Source: Asha and Challapan, 2012)

2.4.3. General security or privacy issues with biometrics

The ability to remain independent, lead your life without any interference and have control over your personal information access is known as privacy (Prabhakar and Pankanti, 2003). According to Neal and Woodward (2016) biometrics does pose three systematic privacy worries:

- Unintended functional scope: Due to the reason that biometric verifications are biological in origin, collectors may glean extra (possibly statistical) individual data from biometric measurements that are scanned. For example, specific misshapen fingers may be associated statistically with specific genetic disorders. With the quick improvements in human genetic studies, fear of extrapolating information from biological measurements may also be a factor in the growth. Medical data derived in this way could develop into a rationale for systemic discrimination against people who are considered to be different from the rest of the population and thus "risky".
- Unintended application scope: Powerful biometric verifications, for instance, fingerprints, permits the likelihood of identifications that are unwelcome. For example, individuals legally maintaining a false or assumed identity (say, for safety reasons) could be verified based on their fingerprints. Moreover, biometric verifications could connect bits and pieces of behavioural information regarding persons enrolled in broadly different applications; detractors regularly construe this potential as a means for organisations - governmental or corporate-to accumulate power over persons and their autonomy.
- Covert recognition: Biometric features are not hidden. It is regularly possible to attain a biometric sample, such as the face of an individual, without his or her awareness. This allows secret recognition of earlier enrolled people. Regrettably, those who admire to remain anonymous in any particular circumstance might be deprived of their privacy by biometric recognition.

2.5. Mobile biometric authentication

A lot research effort has been devoted to the design of more precise, usable, and secure biometric authentication schemes on mobile devices. For instance, Clarke and Furnell (2007) introduced a way for verifying users by encouraging them to insert cell phone numbers or writing messages in the form of a text. This practice is recognised as biometric keystroke analysis.

Kim and Hong (2008) proposed utilising teeth in conjunction with a voice to confirm clients, which became the first study to utilise the teeth and voice combination. The coordinating scores of each person's characteristics are calculated and melded utilising a weighted-summation operation. The tests are conducted by utilising a dataset that includes one thousand teeth pictures and voices collected by smartphones. Afterwards, they proposed an upgraded multimodal authentication framework which incorporates another biometric feature, face, on top of the teeth and voice to acquire greater results (Kim, Chung and Hong, 2010).

Lee, Park, Kang and Park (2009) created a finger-vein and fingerprint-based mobile multimodal biometric system. The proposed system can capture both finger-vein and fingerprint images spontaneously, as well as overcome some of the limitations of unimodal biometric systems, such as lack of precision.

Tao and Veldhuis (2010) came up with a biometric verification framework that is face-based on mobile devices, which contains general information about the method, over and above face detection, authentication, illumination normalisation, registration, and fusion of information.

Chen, Lee and Hsu (2012) suggested a fingerprint-based remote verification strategy utilising mobile devices. In their strategy, both unique marks and secret words are involved to upgrade the level of the security framework. In addition, hashing functions are utilised to execute mutual verification. Kim, Son and Kim (2015) proposed a palm print-based identification framework for mobile devices. A hand-shaped guide window is implemented in particular for quick picture acquisition, and a more competitive code is used to deal with picture variation.

Rattani, Reddy and Derakhshani (2018) made investigations on gender prediction from ocular pictures obtained by smartphones to improve the accuracy of the integrated biometric authentication and mobile healthcare framework.

In the Mobile Iris Challenge Evaluation One contest, Marsico, Nappi, Narducci, and Proenc (2018) compared the results of a few participant strategies. Furthermore, image covariate and interoperability are subjected to review. Several surveys looked at biometric identification procedures on mobile devices, as well as emerging advancement trends and challenges (Marsico, Nappi, Narducci and Proenc, 2018).

2.5.1. Implementation of biometrics on mobile devices

- **Face recognition**

Face recognition applications range from controlled (e.g., mug-shots) to dynamic settings (e.g., airport) (Jain, Ross and Nandakumar, 2004). Face recognition has been applied to surveillance security, border control, forensics, etc. (Spreeuwers, Hendrikse and Gerritsen, 2012). While face recognition is highly studied, its usability and acceptance on mobile platforms has been questionable. A recent survey analysed the opinions of individuals who use, have used, or have never used face unlocking services on capable devices (De Luca, Hang, Zezschitz and Hussmann, 2015). It was found that 36% of the participants considered the service annoying, slow, inconvenient, and difficult to use.

Further, it was felt that capturing facial images for authentication is a socially awkward procedure. Moreover, the group of participants that had never used the service was unaware that it existed on the device, suggesting a lack of manufacturer marketing efforts, while the group that had previously used the service discontinued its use due to usability frustration. Overall, the survey suggested likability with fingerprint recognition due to convenience and positive emotional feedback, such as describing its functionality as ‘fun’ and ‘awesome’. Nonetheless, face recognition is a promising security option for mobile devices. It involves the following steps (Gunther, Shafey and Marcel, 2016):

- Detection: Face detection captures and scales the face.
- Normalisation: The image is geometrically normalised to a fixed resolution, followed by enhancements to reduce the effects of illumination and rotation.

A number of facial recognition databases are publically available, which have allowed a sufficient amount of experimentation on constrained and unconstrained cases (Kasinski, 2008).

However, state-of-the-art performance is restricted to frontal images with limited influences from pose, illumination, expression, and occlusions.

- **Challenges of face recognition**

Face recognition on mobile devices introduces new challenges beyond those traditionally found in non-mobile face recognition systems. An attractive aspect of face recognition on mobile devices is the fact that most users capture photos of themselves while being close to the device. As a result, photographs are typically head shots with direct eye contact. On the contrary, the liberty to take a photo whenever and wherever introduces significant variations between similar photographs, including image blur, angles and/or rotations, varying amounts of background and illumination, and partial images (Fathy, Patel and Chellappa, 2015).

While these are all issues prevalent in most facial recognition applications, mobile devices further complicate this task due to the inability to expect consistent and/or cooperative behaviour. Further, while it is likely that users will be instructed on how to present his or her face during data enrolment, it is very unlikely that this controlled presentation will be reciprocated in the future for authentication as users will expect a fast and casual authentication experience. Moreover, in static face recognition systems, the face is typically captured by the same camera of high calibre for all individuals. On mobile devices, however, the hardware can vary depending on the device. This is especially true for front cameras, which are usually lower in quality compared to the rear. As a result, a universal protocol across all devices may not be a suitable or realistic solution.

- **Periocular**

The periocular area of the face is the surrounding regions of the eyes. Given the availability of high-definition cameras on mobile devices, the periocular region can be reliably extracted from facial images. Periocular recognition is particularly useful when the face is occluded, while the area around the eyes remains available for feature extraction, and a general consensus among researchers is that the periocular region is better suited for biometric authentication compared to other regions of the face (Woodward, Pundlik, Lyle and Miller, 2010). Periocular features can be extracted at two levels:

- Level 1 features are general and holistic, and include attributes regarding eye folds, eyelids, moles, and wrinkles.

- Level 2 features are more detailed, including characteristics such as texture and hair follicles.

The authors continue with periocular recognition via investigation of cross-smartphone performance and introduction of a new feature extraction technique (Raja, Raghavendra and Busch, 2015). Cross-smartphone authentication involves matching between two data samples acquired from different devices.

- **Research challenges**

The periocular area of the face provides an attractive option for biometric recognition. It is easy to capture and contains texture, colour, and shape information, all of which are reliable biometric features. However, on mobile devices, the periocular region is problematic for several reasons. First, periocular recognition suffers from the same problems encountered in face recognition. Beyond this, however, is the fact that occlusions which hinder accuracy in face recognition are likely found in the periocular region, such as eye glasses, hair and hats. Because the user has sole control over the sensor, these occlusions and unpredictable angles and distances from the camera hinder segmentation of the periocular region. Hence, periocular recognition on mobile devices is highly dependent on the user's ability to present a relatively controlled image.

Facial recognition could potentially simplify this process if the algorithm considers several regions of the face as separate components, and can reliably authenticate based on a few regions (for instance, the nose and mouth when the eyeglasses are worn). Periocular recognition, however, leaves very little room for such flexibility, and as a result, an implementation may require inconvenient and unnatural restrictions for adequate use of the service.

- **Fingerprints**

Fingerprints are composed of ridges and valleys found in the skin on the finger tips, where hair and oil glands are not present. Fingerprint features are typically described at three levels:

- Level 1 fingerprint features consist of a ridge orientation map that defines the texture pattern of the finger. Level 1 features identify locations where ridge orientation change, termed loops and deltas. These features are very coarse, and the flow of ridge patterns is visible to the eye under normal circumstances.

- Level 2 features describe the minutiae of the fingerprint, or areas of the ridges that merge, split, begin, and end. Level 2 features appear as an outline, or a single pixel representation, of Level 1 features.
- Level 3 features are the most detailed, and represent sweat pores and the edges of ridges. Capture of Level 3 features requires advanced imaging technology; as a result, these features are typically used only when minutiae are not available, such as in latent, or partial, fingerprints.

Fingerprint recognition has widely established itself as a prominent biometric technology on modern mobile devices for authentication and e-commerce transactions. Apple boasts its fingerprint technology as a "seamless" biometric password, incorporating advanced hardware and software that aids in fingerprint detection, capture, and privacy (Bhagavatula, 2015).

- **Research challenges**

Fingerprint recognition is affected by skin and sensor conditions. For instance, authentication is problematic when fingers are wet or the surface of the device is dirty (Bhagavatula, 2015). Other factors, such as scars and workplace injuries, could complicate data capture and matching (Jain, Ross, and Nandakumar, 2011). Such skin conditions also increase the need for pre-processing, which could add to resource overhead on mobile platforms. For instance, Yamazaki recommends high pass filtering, low pass filtering, ridge direction detection, and ridge enhancement for pre-processing images for brightness normalisation and noise reduction (Yamazaki, 2015). Finally, as currently implemented commercially, after five failed attempts, a user can access the device via a password, thereby subjecting the user to the same disadvantages of a typical knowledge-based system and opening the door for circumvention and adversarial attacks.

- **Palmprint recognition**

Related to fingerprint recognition is palmprint recognition. There is limited research with regard to palmprint recognition on mobile devices; however, while palmprint recognition traditionally required large and expensive palm scanners, advanced imaging from modern smartphones are likely capable of capturing sufficient palmprints for authentication (Corcoran and Costache, 2016). Unfortunately, according to Javidnia (2016), research regarding palmprint recognition on smartphones is limited because of no public, standard dataset. Finally, due to the lack of

constraints in image capture on mobile devices, palmprint applications would have to cope with illumination and rotation variations which are usually addressed in controlled environments through uniform colour backgrounds and finger pegs (Kong, 2009).

- **Iris**

The iris region of the eye arguably provides the most accurate biometric trait (Jeong, 2005). The frontal portion of the iris contains visible muscle which can be captured and used for biometric authentication. The muscles consist of texture patterns which are highly unique and stable over time. Traditional iris recognition systems typically require subjects to present the eye area in a very controlled manner. Several near-infrared images are taken from which a high-quality image is retained (Jain, Ross and Nandakumar, 2011).

Jeong (2005) presents an implementation specifically for mobile devices which employs adaptive Gabor filtering for deriving iris features with the intentions of reducing the processing power needed for authentication.

- **Research Challenges**

There are several challenges associated with iris recognition in general, but these challenges are further complicated on mobile devices. First, the iris is a moving organ inside of another moving organ (the eye) (Jain, Ross and Nandakumar, 2011). Combining this motion with the inevitable movement of the device during data capture creates an immense stabilization problem. Second, iris recognition systems are usually developed for optimal operation indoors (Cho, 2006).

However, mobile devices are used in a variety of environmental conditions. Localisation and segmentation of the iris region in non-ideal lighting conditions is an open research problem. According to Cho (2006) generalising the usual method for iris localisation (i.e., circular edge detection) to mobile platforms is inefficient due to the constant dilation and constriction of the pupil as light conditions change, ghost regions around the iris, and homogeneous grey levels across several components of the eye (Kurkovsky, 2010). These conditions are all observed when the eye is captured outdoors.

Further, near-infrared illumination of the eye is preferred to preserve the iris texture, particularly for dark-coloured irises (Jain, Ross and Nandakumar, 2011). This imposes hardware and usability issues for mobile device users; the device must be equipped with a near-infrared sensor,

the user must be cautious of the distance between the eye and the sensor to avoid any eye damage and the user must actively cooperate with the system for adequate data capture.

Finally, the iris region is described as a "stochastic texture containing numerous edges like features that are randomly distributed" (Jain, Ross and Nandakumar, 2011). This implies the need for sophisticated modelling algorithms which have the potential to overwhelm the device's resources. Traditionally, iris recognition involves several steps beyond localisation and segmentation, including normalisation, encoding, and quality assessment, all of which are expensive mathematical processes.

- **Keystroke dynamics**

Keystroke dynamics are a cost-effective solution to biometric authentication on mobile devices (Karnan, 2011). Additional hardware is not required. Given that a user must operate the device via key input, continuous authentication is feasible and typing behaviour is unique. Recognition via keystroke dynamics involves the analysis of keystrokes and typing patterns (Saini, 2016). Common features include:

- Key press/down, or the time of a key press event.
- Key release/up, or the time of a key release event.
- Latency, or the time from press-to-press, release-to-release, or release-to-press events.
- Hold time, or the duration of a key press event (i.e., how long the key was pressed).
- Pressure or the measurement of the finger's pressure on the screen.
- Size or the area of the screen pressed by the finger.
- Error rate, or the number of times the user presses a backspace or delete key due to erroneous input.

Analysis of keystroke dynamics has a traditional application on computers with similar features (Monrose and Rubin, 2000).

- **Research challenges**

There remains a need for performance evaluations under uncontrolled conditions, such as typing while walking or lying down. A user may type differently according to his or her emotional or physical state. Injuries to the hands, temporal changes to the device's screen, and even changes

in typing speed could result in performance degradations. These are all non-trivial scenarios that are most likely the future of keystroke dynamics for mobile device security (Saini, 2016).

2.5.2. Benefits of mobile biometrics

Mobile biometrics, most of the advantages of classical biometrics, endorsing its resources. Advantages linked with mobile biometrics include the following:

- Portability: Due to the compactness and portability, these devices allow authentication at any time and in any place.
- Effectiveness of cost: Due to sensor advancement and increasing computational control of the processing units installed in the devices, the cost of performing biometric verification on mobile devices is usually low.
- Popularity of market and consumer acceptance: Due to popularity and wide utilisation of mobile devices, the simplicity of use, as well as the acceptance of both consumer and industry have increased (Toledano, Pozo, Trapote and Gomez, 2006).

2.5.3. The future of mobile biometrics technology

Lakshman (2018) said that after desktop, Kiosk, ATM and IoT systems will be the next boundary for biometrics. Like the WhoYou.co.za as a website example, these devices can identify clients through biometric authentication that is pushed as a notification on their mobile phones. Imagine using an ATM where a debit card is not needed. Alternatively, the registered smartphone on your account would receive a fingerprint scanning notification or iris to process the transaction (Lakshman, 2018).

2.5.4. Challenges and open issues of mobile biometrics

According to Jo (2016) security and privacy are important aspects of biometrics on mobile devices. Clients must be certain that their biometric characteristics are shielded from sources outside and used for the planned purpose for them to be widely accepted. Unfortunately, antagonistic attacks such as spoofing through the use of images during the detection of face and fingerprint moulds make biometric systems vulnerable.

.

It has been demonstrated, for example, that before security updates, malware that can obtain the fingerprint image stored in the device's local memory, remove the fingerprint prototype, and restore the fingerprint features may be developed (Jo, 2016). Much research has gone into avoiding such accidents in traditional biometric systems; these, as well as modern applications, are now being extended to mobile platforms.

2.5.4.1. Challenges of mobile biometrics

There are four issues with mobile biometrics that have been discovered. These incorporate acquisition, pre-processing, feature extraction and template storage (Reddy, Rattani and Derakhshani, 2016). The sensors installed in mobile devices, specifically smartphones, are limited in size and cost with acquisition. The former is of pertinence specifically for biometric features like fingerprints, palm-prints, finger and hand veins. Additional components concern the quality and heterogeneity of mobile-inserted microphones, which affect a voice-based framework (Reddy, Rattani and Derakhshani, 2016). Sensor resolution is related to the number of acquired features and it may affect the accuracy of a biometric system based on face or, more precisely, on the iris.

The second one is pre-processing. Once attained, biometric examinations pass through a pre-processing stage that seeks to select from the data raw only the information compulsory for matching biometrics. This step may consider segmentation, reduction of noise, as well as colour and shape normalisation. In the case of mobile iris recognition, for example, segmentation has always been a challenge, specifically in the visible spectrum (Frucci *et al*., 2014 and Reddy, Rattani and Derakhshani, 2016).

Thirdly, technical advancements in feature extraction have greatly reduced the computational power gap between traditional and mobile-based systems. Nonetheless, a mobile device's resources are limited, and algorithms must be tailored to suit them. This raises the issue of how to use memory and computationally intensive approaches including deep neural networks (Qualcomm, 2018).

Finally, template storage. If processed biometric user information is encrypted and stored within mobile devices, it is usually easy for an adversary to obtain the processed data if the phone can be retrieved (Wojciechowska, Chora´s, and Kozik, 2017). Unlike traditional biometric

frameworks, which are manipulated and monitored only by approved staff (e.g., spying videos), mobile devices are entirely under the control of the user. This security challenge necessitates the use of advanced encryption techniques to protect biometric information that is processed, as well as the use of detection of a presentation attack to prevent impostors from gaining access.

2.5.4.2. Open issues

Biometric authentication is repeatedly regarded as a more secure approach than knowledge-based authentication for some reasons that were found to be obvious: biometric traits are unforgettable or cannot be stolen, and they are difficult to spoof (Neal and Woodard, 2016). These advantages, however, do not imply a faultless and seamless authentication method (Neal and Woodard, 2016). There is a necessity to deal with current issues immediately so that every individual can welcome and use technology. It is important to address open problems as soon as possible so that everyone can embrace and use technology. As a result, this paper identifies many problems in a biometric system that continue to be a snag in terms of accuracy, generalisation, and adaptability. Aside from template security, there are four unique research challenges with mobile devices that have proven difficult to overcome: these incorporate hardware limitations, environmental and user-induced noise, inconsistent data and balancing transparency (Neal and Woodard, 2016).

- **Hardware limitations**

According to Neal and Woodard (2016) persistent user access to the sensor is a major problem in terms of hardware. Furthermore, in conventional biometric systems, users only interact with the sensor briefly. Nonetheless, on mobile devices, the general element of the device's architecture is the sensor, with no protections in place to avoid tampering and spoofing (Neal and Woodard, 2016). Having said that, how to appropriately protect the sensor of the device without impeding its intended activity beyond biometric authentication remains an open issue.

Furthermore, the specifications of hardware differ from one computer to another. While one biometric modality may be appropriate for one application, the sensor required by that modality may not be available on other platforms. This necessitates platform-specific implementations (Neal and Woodard, 2016). As a final point, some modalities can incur extra hardware costs, decrease the device's convenient, or necessitate more storage or processing power. Usability and

portability are important features of mobile devices, but biometric technology has the ability to drastically minimise the device's daily operation (Neal and Woodard, 2016).

- **Environmental and user-induced noise**

Environmental factors like scenes in the background, lightning and additional sources of noise all have an effect on the ability to collect a sample of high-quality. Such influences necessitate segmentation algorithms to distinguish the true biometric feature from noise caused by the environment noise (Anil and Jain, 2016).

In addition, modality-specific noise, make-up, finger cuts on, facial recognition accessories and illnesses affecting the tract of vocal in speech recognition all pose a challenge. As a result, although the biometric feature can be accurately captured, the sample contains noise that reduces accuracy (Anil and Jain, 2016).

Denoising strategies such as Principal Component Analysis may help reduce noise, but other challenges include determining how to discriminate between noises, distinguishing information and balancing the computational burden on resource-constrained mobile devices when putting those algorithms into action (Anil and Jain, 2016).

Furthermore, there is little research on how to suitably measure quality of data, identify when a sample is bad and advise the participant on how to display himself or herself to the sensor so that appropriate data collection can take place (Committee, 2010).

- **Inconsistent data**

Inconsistencies in data samples are caused by physical and/or behavioural differences, which typically lead to poorer samples of data quality or poor matching. Changes that are unavoidable, such as aging and disease are examples of physical differences (Anil and Jain, 2016). The aging effects are visible virtually in all biometric modalities and identifying the same topic over long periods is a major research challenge (Anil and Jain, 2016). Behavioural changes, instead, are more easily persuaded by emotions and consist of changes in behaviour of typing and facial expression. When such differences are added, inconsistencies between the probe features and gallery are possible.

- **Balancing transparency**

Adaptability users can find physiological modalities inconvenient because they require the same number of authentication efforts as knowledge-based techniques. These characteristics often fail to offer consistent and straightforward security (Abdulwahid, 2016). In behavioural frameworks, on the other hand, there is a lack of clarity due to the inability to check when the user is not presenting the details that the mechanism is designed to control. Since human behaviour is sporadic, it seems that relying exclusively on a behavioural system is impossible (Abdulwahid, 2016).

2.6. Conclusion

It is significant to take into consideration that consumer acknowledgment and certainty are very important for the advancement of a method or an idea. Technology acceptance is defined as an information systems theory that models how users come to accept and use technology. Mobile technologies have entered the realm of interest of researchers in different scientific disciplines. A part investigates physical or mental effort has been devoted to the plan of more exact, usable and secure biometric verification plans on mobile devices. Mobile biometrics have a significant portion of the advantages of traditional biometrics, thus supporting its capabilities. Clients should be certain that their biometric distinctive attributes are shielded from outside sources and utilised for the planned reasons for them to be widely accepted. In a biometric method, many issues stay a snag in terms of accuracy, generalisation, and adaptability. Kiosks, ATMs, and IoT systems will be the next frontier for biometrics.

Chapter three: Research design and methodology

3.1. Introduction

Chapter two explored the literature review. The historical background and theories of different researchers were sourced to develop a clear understanding of what mobile biometric devices are all about. This chapter gives a general description of the methodology that was followed to investigate the research questions to find a possible solution for the research problem. This incorporates a detailed discussion of the philosophical background of the research method chosen. Moreover, this chapter describes the strategies used for data collection and the selection of research instruments and sampling. This chapter will start by presenting the case study research design for the current study as shown in Figure 3.1.

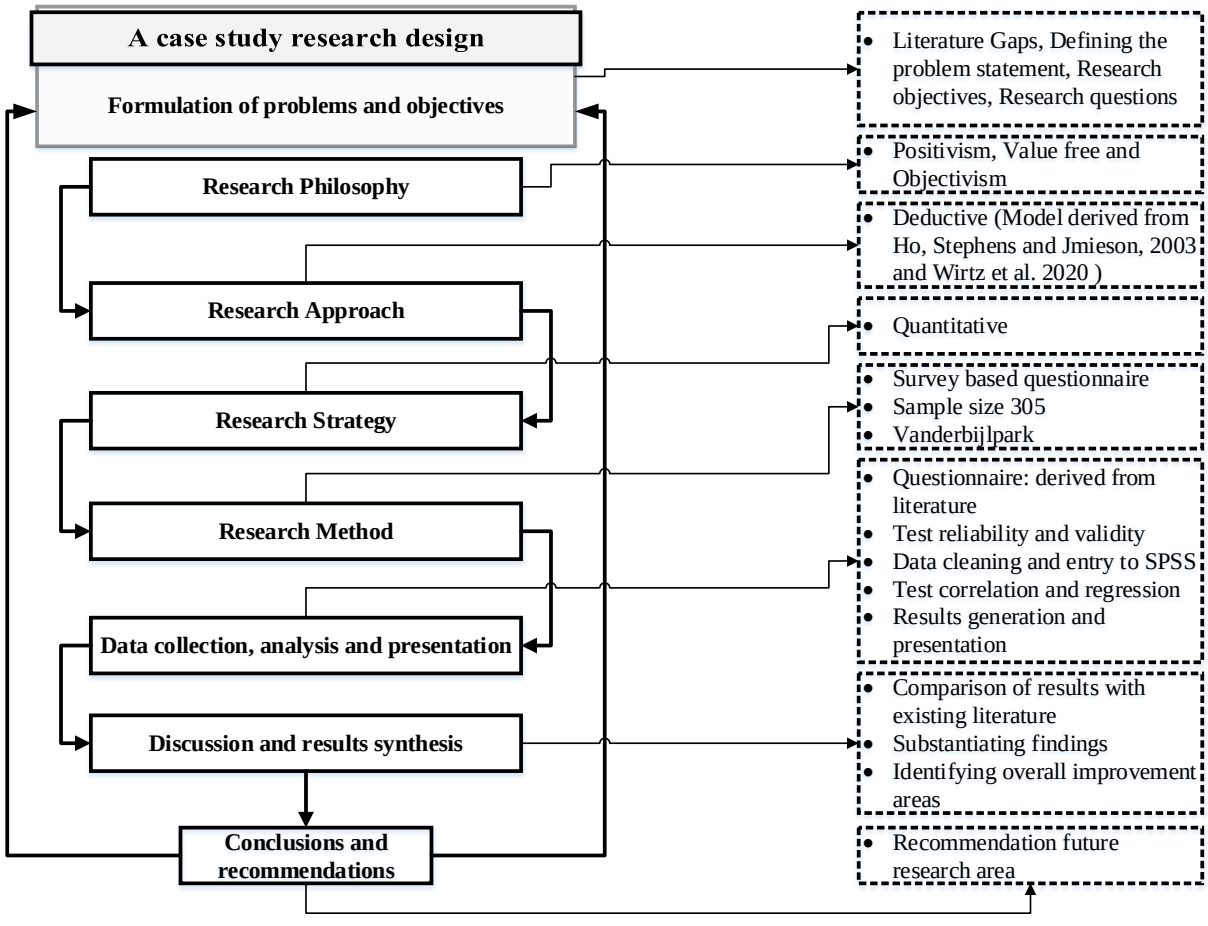


Figure 3. 1 A case study research design for the current study

3.2. Research problem

3.2.1. Defining the problem

In recent years, mobile device access to information has become commonplace in both business and personal settings. The world is turning out to be technically connected, and all mobile users need to know that their data is secure (Kadena and Ruiz, 2018). Biometric technology is preferred to improve the security of mobile devices and the efficiency of wireless networks (Clarke and Furnell, 2005).

Many studies have been conducted on biometric devices and application adoption, consumer attitudes toward these devices, and performance effect measurements. That being said, only a few of the studies have looked into the factors that have an influence on biometric device acceptance (James *et al*., 2017). According to Chau, Stephen, and Jamieson (2004), of the few studies that were undertaken to assess biometric technology acceptance, only a small number were performed on the issues faced by users concerning biometric acceptance and use

There were also just a few studies that focused on the acceptance of biometric authentication technology on mobile devices. Since mobile devices are used for both business and personal purposes, this study sought to determine the level of acceptance of biometric authentication technology on mobile devices.

3.2.2. Aims and objectives of the current study

The primary goal of this study was to determine how biometric authentication technology on mobile devices was perceived. The following goals were used to accomplish the main goal:

- To study and determine what was done, according to the literature to measure user acceptance of technology.
- To propose a model that can be used to measure the acceptance of biometric authentication technology on mobile devices.
- To measure the effect of every variable of the model in the acceptance of biometric authentication technology on mobile devices.

3.2.3. Research questions of the current study

The main research question of this study was: What is the perception of acceptance of biometric authentication technology on mobile devices? This main research question was answered through the following secondary research questions:

Secondary research questions

- What has been done, according to the literature to measure user acceptance of technology?
- What model can be proposed to measure the acceptance of biometric authentication technology on mobile devices?
- How does one measure the effect of every variable of the model in the acceptance of biometric authentication technology on mobile devices?

3.3. Research philosophy

The most significant part of the research methodology is called research philosophy (Saunders, Lewis and Thornhill, 2012). Research philosophy is a specific way of expanding knowledge that describes the philosophical paradigm (Saunders, Lewis and Thornhill, 2012). It is categorised as ontology, epistemology and axiology. The above mentioned philosophical techniques allow researchers to make decisions on which technique should be adopted and the reasons it should be adopted, which is obtained from research questions (Saunders, Lewis and Thornhill, 2012). It involves the intersection of philosophy, research design and particular methods shown in Figure 3.2 below.

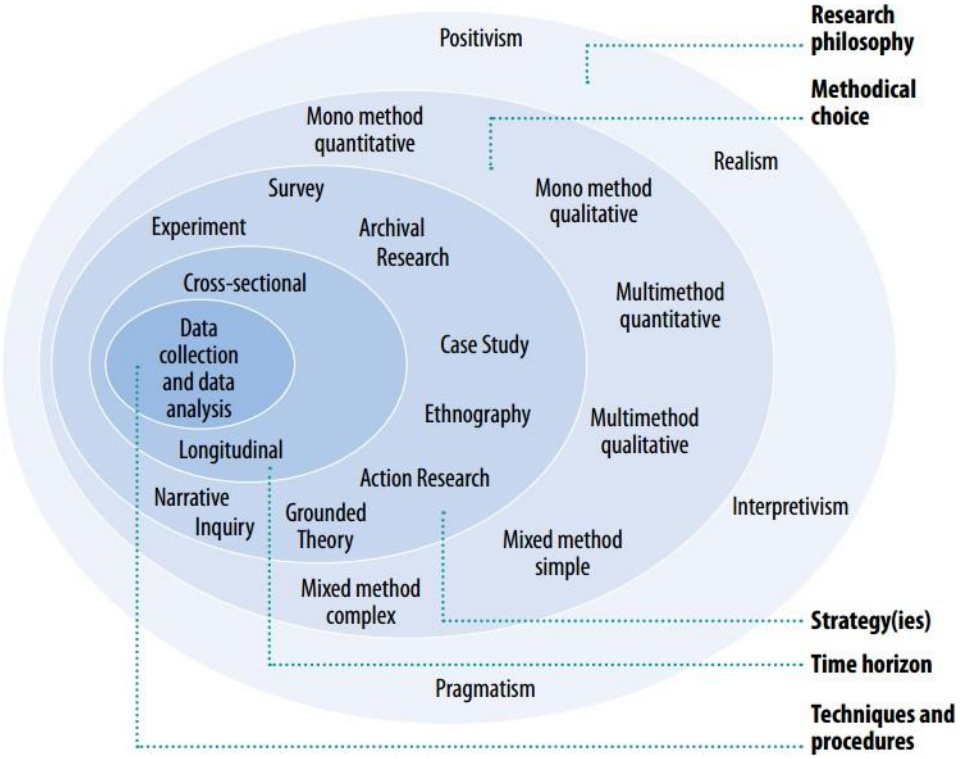


Figure 3. 2 Research Onion (Source: Saunders and Tosey, 2013)

The researcher's opinion about the world is described by significant assumptions that exist in research philosophy. These existing assumptions will define the research strategy and the procedures of that strategy (Saunders, Lewis and Thornhill, 2012). Saunders, Lewis and Thornhill (2012) highlighted that there are three various types of research philosophy. These research philosophies are explained below:

3.3.1. Ontology

Ontology is one of the three types of research philosophy. It can be described as "the science or study of being" and it deals with the nature of reality (Berryman, 2019). Moreover, ontology is a system of beliefs that reflects an interpretation by an individual regarding what constitutes a fact (Berryman, 2019). There are two significant aspects of ontology. These aspects include objectivism and subjectivism (Saunders, Lewis and Thornhill, 2012).

3.3.1.1. Objectivism

Objectivism claims that social objects continue to exist in reality external to social actors (Kothari, 2012). It is alternatively an ontological position that maintains that social circumstances and their definitions have an existence that is not dependent on social actors (Kothari, 2012).

3.3.1.2. Subjectivism

Subjectivism is the second aspect of ontology. It is concerned about the social circumstances which are developed from the perspectives and outcomes of those social actors concerned with their existence (Sobh and Perry, 2006). Subjectivism can formally be described as the ontological position which maintains that social circumstances and their definitions are being continuously achieved by social actors (Bryman, 2012).

3.3.2. Epistemology

Epistemology is the second type of research ontology. It is the part of philosophy that is concerned with nature, the limits of human knowledge and origin (Berryman, 2019). According to Berryman (2019), epistemology can be divided into two parts: resource researcher and feeling researcher. The resource researcher focuses on data from the perspective of a natural scientist whilst a feeling researcher focuses on the feelings and attitudes of the employees towards their managers (Berryman, 2019). Epistemology is classified as realism, positivism, pragmatism and interpretivism in the domain of research philosophy (Saunders, Lewis and Thornhill, 2012).

3.3.2.1. Positivism

The philosophical technique of the natural scientists is seen in positivism as the task of the natural science is based on observable social entities (Corry, Porter and McKenna, 2018). During hypothesis development and data collection, a research strategy is approached. Hypothesis testing will be done to confirm which one can be used for future research (Corry, Porter and McKenna, 2018). Another characteristic of this philosophy is that the positivist researcher is guided by a highly structured methodology to facilitate the hypothesis (Corry, Porter and McKenna, 2018). Moreover, positivism works on quantifiable observations and accordingly statistical analysis is obtained (Soiferman, 2010).

3.3.2.2. Interpretivism

Interpretivism is a part of epistemology that concentrates on the evaluation of the differences between beings as social actors (Saunders, Lewis and Thornhill, 2012). This technique is focused on social world life and the variation between the modern approach and the interpretivism approach (Saunders, Lewis and Thornhill, 2012).

3.3.2.3. Realism

Realism is another philosophical part of epistemology which associates with a scientific question. The main characteristic of realism is related to revealing the truth of reality and the existence of the objects is dominant independently of the human mind (Jebreen, 2012).

3.3.2.4. Pragmatism

Pragmatism uses both positivism and interpretivism philosophy and sees both of them as a continuum instead of contradictions (Creswell, 2013). Appropriately pragmatism prevents getting involved in argumentative concepts of reality and truth (Creswell, 2013).

3.3.3. Axiology

Axiology is the third type of philosophy that is concerned about judgments, aesthetics and ethical approaches (Saunders, Lewis and Thornhill, 2012). The procedure of social inquiry is involved in this technique. The researcher's axiological skill is implemented in order to make judgments regarding the research content and its conductive approach (Saunders, Lewis and Thornhill, 2012).

For the purpose of this study, positivism, objectivism and value-free philosophies were chosen since they involve highly structured hypothesis testing and statistical tools and were also proven to be suitable for quantitative research studies (Holden and Karsh, 2009; Saunders, Lewis and Thornhill, 2012; Sobh and Perry, 2006; Kothari, 2012).

3.4. Research approach

There are numerous commonly used approaches for carrying out research studies. These approaches are categorised into deductive research approach and inductive research approach (Welman, Kruger and Mitchell, 2015). A deductive research approach focuses on the development of hypotheses based on an existing theory and designing a research strategy to put those hypotheses on a test (Wilson, 2010). According to Gulati (2009), deductive refers to reasoning from the particular to the general. In order to check if a link or a relationship obtained more or general circumstances, a deductive design is deployed (Gulati, 2009). Figure 3.3 illustrates some processes of the deductive research approach.

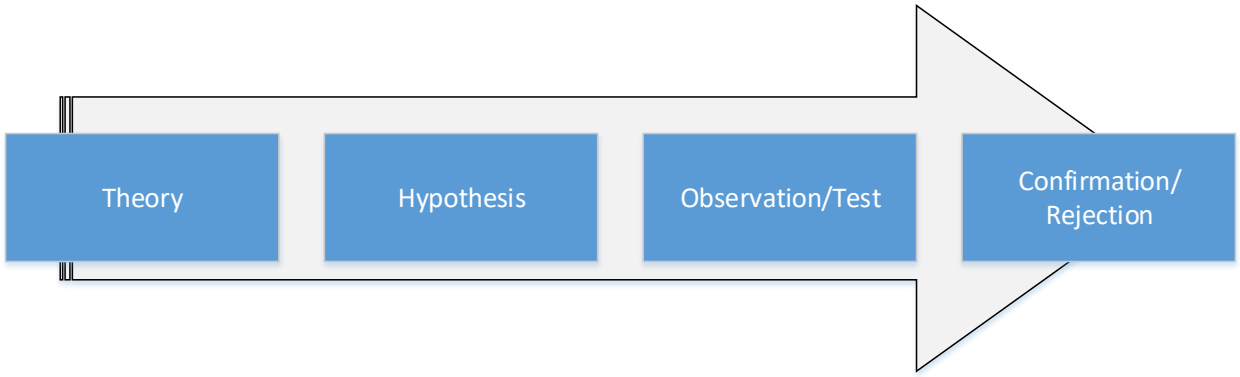


Figure 3. 3 Processes of deductive research approach (Source: Pelissier, 2008)

According to Babbie (2010) advantages of the deductive research approach include the following:

- Capability of describing causal links between concepts and variables.
- Capability of measuring abstract ideas quantitatively.
- Capability of generalising research results to a particular degree.

According to Pelissier (2008), studies that are conducted using the deductive approach consist of the following four stages:

- Deducing hypothesis from theory.
- Formulation of hypothesis in operational terms and suggesting relationships between two particular variables.
- Hypothesis testing with relevant applicable methods (quantitative methods such as

correlation analysis, regression analysis, means, modes, medians, etc.).

- Evaluating the results of the test and therefore affirming or rejecting the theory.
- Modifying theory in situations whereby a hypothesis is not confirmed.

Inductive research approach is the second approach used for carrying out a research study. An inductive research approach or inductive reasoning begins with the observations and then later towards the end of the research process theories are suggested as outcomes of observations (Goddard and Melville, 2004). Inductive studies do not apply hypotheses or theories at the beginning of the study and the researcher is free to alter directions for the research at the end of the research process (Benard, 2011). According to Saunders, Lewis and Thornhill (2012), the inductive approach is based on learning from experience. Figure 3.4 illustrates some processes of the inductive research approach.

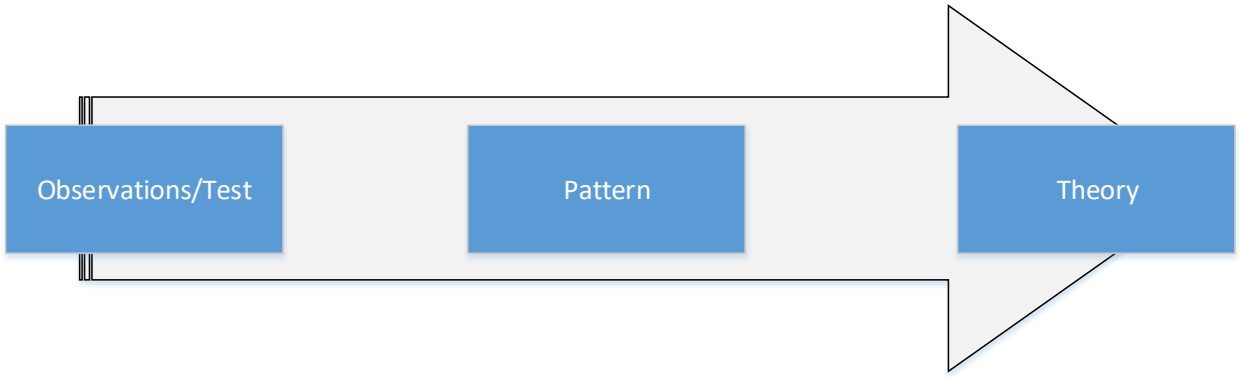


Figure 3. 4 Processes of inductive research approach (Source: Lodico, Spaulding and Voegtle, 2010)

The deductive research approach was chosen for this study as it is capable of describing causal links between concepts and variables; moreover, it is capable of measuring abstract ideas quantitatively (Babbie, 2010). It was selected for this analysis because it had previously been used in similar studies and had proved to be suitable.

3.5. Research strategy

Research strategy is the plan for carrying out research (Newcastle, 2019). It consists of three types of data-gathering techniques, each of which utilises a different method. Those techniques are qualitative, quantitative as well as mixed method (Newcastle, 2019).

3.5.1. Qualitative research

Qualitative research gathers information about people's living experiences, emotions, and behaviours, as well as the meanings they place on them. It aids researchers in gaining a greater understanding of difficult ideas, social dynamics, or culturally significant changes (Newcastle, 2019). This type of study is useful for determining how or why things happened, as well as analysing the results (Newcastle, 2019). For this method, the following procedures or tools can be used to collect research data:

- Interviews: In-depth interviews, unstructured or semi-structured between the interviewer and a participant may be held (Newcastle, 2019).
- Focus group: A group of people discussing a specific topic or a series of questions. Researchers may either be organisers or observers (Newcastle, 2019).
- Observations: part-play observations, in-setting, or on-site (Newcastle, 2019).
- Analysis of document: interrogating correspondence (literature, papers, emails, etc.) or reports (Newcastle, 2019).
- Speech history or life stories: Reminiscence or recall of information provided to the researcher (Newcastle, 2019).

Using qualitative analysis techniques and methods has several advantages. To begin, qualitative research yields a dense (detailed) summary of participants' thoughts, viewpoints, and experiences (Denzin, 2002). Second, qualitative research allows researchers to learn about the participants' inner lives and how meanings are influenced by and within society (Corbin, 2008).

Beyond the benefits, there are clear drawbacks. First, according to Silverman (2010), qualitative research methods often overlook contextual sensitivity in favour of focusing on definitions and perceptions. Second, the findings of a qualitative approach could be viewed with scepticism by policymakers.

3.5.2. Quantitative research

Bryman (2012) describes quantitative research as "A research strategy that emphasises quantification in the collection and analysis of data". The tools or techniques utilised for gathering research data for this method comprise:

- Questionnaire: This type of survey asks similar questions to a large number of people or uses scales to assess people's opinions or feelings as statistical data (Bryman, 2012).
- Observation: This can be either counting the number of times a given event occurs or coding the observed data to translate it into numbers (Bryman, 2012).
- Screening document: obtaining statistical data from financial reports or recording the number of times a term appears in a document (Bryman, 2012).
- Experiments: in-lab testing of theories, effect testing, and effect relationships, through field experiments or quasi- or normal experiments (Bryman, 2012).

Using quantitative analysis techniques and methods has several advantages. The quantitative results are commonly generalised to the whole population or a sub-population because it contains the greater sample which is chosen randomly (Carr, 2009). The positivist paradigm of evaluating variables is then to be used in quantitative analysis (Kauber, 2011). The quantitative analysis approach, like any other, has benefits and drawbacks. To begin with, a quantitative analysis methodology tends to take a glimpse of a phenomenon. Second, positivism is incapable of explaining how social reality is influenced and preserved, or how people perceive their own and others' behaviours (Blaikie, 2007).

3.5.3. Mixed methods

In a single study or series of studies, a mixed approach focuses on gathering, evaluating, and combining both quantitative and qualitative data. Its basic concept is that combining quantitative and qualitative methodologies yields a greater understanding of research issues than either methodology alone. The following are the characteristics of this method (Newcastle, 2019):

- Gather and analyse quantitative as well as qualitative data.
- Combine two types of data in various ways.
- Give one or both types of data precedence.
- Can be included in a single analysis or several phases of one.

IRB questions, decisions about who to survey, decisions about which quantitative findings require more clarification, what parameters were used for sample selection for a qualitative study and time-consuming are some of the challenges of using mixed methods in research (Newcastle, 2019).

A quantitative research method was chosen for this study as this strategy needs a more ethical science based on probability obtained from the study of large numbers of randomly chosen cases (Welman, Kruger and Mitchell, 2015). The quantitative study depends on the numerical data collection and analysis to give a detailed description, foretell, explain or manage variables and interest phenomena (Gay, Mills and Airasian, 2009).

When carrying out quantitative studies, researchers attempt to provide a detailed description of the current circumstances, demonstrate existing relationships among variables, and at times try to clarify casual associations among variables (Creswell, 2005). This type of study operates under broadly agreed-on procedures that provide direction to the research process (Fraenkel, Wallen and Hyun, 2012). According to Creswell (2005), the main aim of the quantitative study is for the researcher to keep as objective as possible.

3.6. Research design

There are numerous commonly used research designs for carrying out quantitative research studies. These approaches are categorised into non-experimental research design and experimental research design (Welman, Kruger and Mitchell, 2015). Non-experimental research design includes a group of methods used to carry out quantitative research where variables are not manipulated anywhere in the study (Welman, Kruger and Mitchell, 2015). In a non-experimental research design, variables are being measured the way they occur without the intrusion of any type by the researcher (Welman, Kruger and Mitchell, 2015).

Experimental research design is the second approach used for carrying out a quantitative research study (Welman, Kruger and Mitchell, 2015). This is a group of methods where the researcher determines various treatments or situations and then studies their effects on the participants (Welman, Kruger and Mitchell, 2015).

A non-experimental research design was chosen for this study as it utilises the structured method to appraise objective data consisting of numbers and may be carried out in natural environments such as workplaces and business buildings (Welman, Kruger and Mitchell, 2015). It was chosen for this study because it has been shown to be suitable in previous similar studies.

3.7. Research methodology

The specific measures or methods used to define, select, process, and analyse knowledge about a subject are referred to as research methodology (Wits, 2019). The methodology section of a research paper allows the reader to objectively evaluate a study's general validity and accuracy (Wits, 2019). Two key questions are addressed in the methodology section: What methods were used to collect or generate the data? What method was used to examine it? (Wits, 2019).

3.7.1. Research methods

Procedures or techniques used in the collection of data or evidence for analysis in order to find out current knowledge or obtain a deeper understanding of a study are referred to as research methods (Newcastle, 2019). There are numerous existing research methods that can be implemented in a study as shown in figure 3.1. Moreover, a quantitative research strategy on its own has many methods available (for example, web-based surveys, postal surveys, telephone interviews and structured questionnaires) (Haq, 2014). Every single instrument of the above mentioned has its own advantages and disadvantages associated with it in terms of cost of data, time and quality (Haq, 2014).

Brymand (2006) and Driscoll, Yeboah, Salib and Rupert (2007) note that many researchers prefer structured questionnaires for data collection and they are unable to manage or influence respondents which results in lower rates but more accurate data obtained. However, Saunders and Tosey (2015) maintained that quantitative data is easier to obtain and briefer to present. Thus, a survey-based questionnaire was chosen for the current study as it has proved to be suitable in related studies.

3.7.2. Justification for the use of a survey-based questionnaire

Surveys are taken into consideration as one of the most traditional ways of carrying out a study and are useful in non-experimental descriptive designs that need to define some kind of reality (Kelly, Clark, Brown and Sitzia, 2003). Survey-based questionnaires are frequently limited to a representative sample of a potential group that constitute the researcher's interest (Kelly Clark, Brown and Sitzia, 2003). The survey instrument was chosen for its effectiveness at being practical and less costly (Kelly Clark, Brown and Sitzia, 2003). Because of the philosophical assumptions, the survey design is considered the best instrument that is in line with these premises in addition to being cost effective.

3.8. Population and sampling

3.8.1. Population

A research population can be defined as a group of individuals, objects and institutions with similar characteristics or features that are of interest to a researcher. The similar characteristics differentiate them from other institutions, objects as well as individuals (Ouedraogo, 2020). The population of this study was Vaderbijlpark citizens in South Africa, Johannesburg consisting of all races, educational status, age groups and employment status.

3.8.2. Sample

A sample can be described as a small portion of the population chosen for particular research (Taherdoost, 2016). According to Taherdoost (2016) the sample should signify the characteristics of the proposed group. For the purpose of this study, a subset of 305 citizens was chosen to represent the entire population of mobile users in Vanderbijlpark Johannesburg.

3.8.3. Sampling

Sampling can be described as a procedure for choosing or drawing the exact representation of a group unit or sample from a population of interest (Taherdoost, 2016). For this study, a simple random sampling technique was chosen as it was meant to be an unbiased representation of a group and is a subgroup of a statistical population in which every one of the subgroups has an equal probability of being chosen (Adam, 2019). All participants of this study were randomly chosen without been grouped into categories.

3.8.4. Sampling frame

The sampling frame can be described as a list of subjects or people who will form part of the study (Taherdoost, 2016). For the purpose of this study, students (both postgraduates and undergraduates) with different educational status, employed citizens, unemployed citizens, self-employed citizens, retired citizens, of different age groups and gender and different races were chosen.

3.8.5. Sample size

Explorable (2009) describes the sample size as a term used in market research for defining the number of subjects included in a sample. For this study, a total number of three hundred and five (305) participants were chosen because most related studies in the literature review used this number and the sample target was three hundred (300) participants. Fifty-one (51) questions were given to each participant to answer.

3.9. Data collection

According to Vuong and Trang (2018) data collection is the process of gathering and analysing information on target variables in a standardised structure, allowing appropriate questions to be asked and the results to be assessed. Furthermore, according to Vuong and Trang (2018), data collection is an important part of all fields of research, including the physical and social sciences, as well as industry.

The items that were used to collect data for this research in the survey questionnaire were built from the review of the existing and past literature that is relevant to the model of this research. A five-point Likert - scale measurement type from one "strongly agree" to five "strongly disagree" was utilised in this research. After the development of the questionnaire, a pilot study was carried out with 30 participants (10% of the sample size) to ensure good length of questions, good clarity of the instruments, and content completeness.

The questionnaire was divided into two distinct sections. The first section of the questionnaire aimed to collect background information which included questions associated with demographics, user experience of information technology, the use of the internet and user experience of internet scams. The second section of the questionnaire aimed to find out the

perception of use of mobile biometrics. The questionnaire of this study was created based on the research framework derived from Ho, Stephens and Jamieson (2003). The following constructs were posited in the questionnaire shown in Table 2:

- Perceived Usefulness
- Perceived Ease of Use
- Subjective Norm
- Trust
- Perceived Humanness
- Perceived Interactivity
- Perceived Social Presence
- Actual Use of Biometric Mobile Device
- Accuracy
- Identity Theft
- Reliability
- Privacy
- Security
- Identity Assurance
- Combining Data
- Intention to Use

Table 3. 1 Survey questionnaire and related variables

Code	Construct	Measuring Item	Hypothesis	Source-citations
PUse1	Perceived Usefulness	Using a mobile biometric device in my job would enable me to accomplish tasks more quickly	H_{05}, H_{08}, H_{09}, H_{11}	(Emily,Johnson and Carmen, 2019)
PUse2		Using a mobile biometric device would improve my job performance.		
PUse3		Using a mobile biometric device would enhance my effectiveness on the job.		
PUse4		I would find a mobile biometric device useful in my job and for personal use.		
PEofU1	Perceived Ease of Use	My interaction with a mobile biometric device would be clear and understandable.	H_{04}, H_{08}, H_{10}	(Emily, Johnson and Carmen, 2019)
PEofU2		I would find a mobile biometric device to be flexible to interact with.		
PEofU3		Learning to operate a mobile biometric device would be easy for me.		
PEofU4		I would find a mobile biometric device easy to use.		
SubN1	Subjective Norm	People who influence my behaviour think that I should use the mobile biometric device	H_{06}	(Barbara, Belanger and Schaupa, 2017)
SubN2		People who are important to me think that I should use a mobile biometric device.		
SubN3		I use the mobile biometric device because of the proportion of people around me who also do.		
SubN4		People around me who use the mobile biometric devices have more prestige than those who do not		
Trs1	Trust	I do not doubt the honesty of a biometric mobile device	H_{13} H_{14} H_{15} H_{07}	(Cheng, Sun, Bilgihan and Okumus 2019)
Trs2		The mobile biometric device will keep my data private.		
Trs3		The mobile biometric device will keep my data secured.		
Trs4		The mobile biometric device will ensure reliable security for my device.		

PHum1	Perceived Humanness	I am happy about a mobile biometric device.	H_{01}	(Lankton, Knight and Tripp, 2015)
PHum2		I am satisfied with a mobile biometric device.		
PHum3		I understand a mobile biometric device.		
PInt1	Perceived Interactivity	If I can easily unlock my mobile biometric device without any delay.	H_{02}	(Gao, Rau and Salvendy, 2009)
PInt2		If I will have a lot of control over my mobile biometric device.		
PInt3		If there will be good communication between me and my mobile biometric device.		
PSPst1	Perceived Social Presence	There is a sense of sociability with a mobile biometric device.	H_{03}	(Lankton, Knight and Tripp, 2015)
PSPst2		There is a sense of human warmth with a mobile biometric device.		
PSPst3		There is a sense of human contact with a mobile biometric device.		
AUofBMD1	Actual Use of Biometric Mobile Device	I have used a mobile biometric device before.	H_{12}	(Asiimwe and Orebro, 2015)
AUofBMD2		I have used a mobile biometric device for too long.		
AUofBMD3		I often use a mobile biometric device.		
Acry1	Accuracy	I thought there was too much consistency in this mobile biometric device.	H_{10}	(Tullis and Stetson, 2004)
Acry2		I found the various functions in the mobile biometric device well integrated.		
ITht1	Identity Theft	I am afraid that somebody can unlock my mobile biometric device easily.	H_{16}	(Jordan, Leskovar and Maric, 2018)
ITht2		I am very worried that the unauthorised use of my personal data from my mobile biometric device can damage my reputation.		
Rbty1	Reliability	I find biometric security reliable enough to protect my mobile device.	H_{13}	(Tuunainen, Pitkanen and Hovi, 2009)
Pry1		I worry about my data privacy while using the mobile		

	Privacy	biometric device.	H_{15}, H_{16}, H_{17}	(Tuunainen, Pitkanen and Hovi, 2009)
Pry2		I feel that the privacy of my personal information is protected by biometric security on my mobile device.		
Sty1	Security	I worry about my data security while using a mobile biometric device.	H_{14}	(Tuunainen, Pitkanen and Hovi, 2009)
Sty2		I'm familiar with data protection and securing while using mobile biometrics in general.		
IAnc1	Identity Assurance	Each user of mobile biometric device will have unique user traits.	H_{11}	(Jordan, Leskovar and Maric, 2018)
IAnc2		The user traits will match my biometric user filed.		
Cdt1	Combining Data	I do not have any concern about biometric security responsible for combining my login details on my mobile device.	H_{17}	(Oishi, Kurokura and Yegi, 2019)
ItoUse1	Intention to Use	I intend to use a mobile biometric device in my class or workplace.	H_{01}, H_{02}, H_{03}, H_{04}, H_{05}, H_{06},H_{07}, H_{12}	(Weng, Yang, Ho and, 2019)
ItoUse12		I increase the occurrence of using a mobile biometric device in class or workplace.		

3.9.1. Validity

Validity can be described as a measure of truth or falsity of the collected data through research instruments. It can be categorised into internal and external validity of the assessing instrument (Golafshani, 2003). In the current study, validity refers to the measure of truth or falsity of the assumed acceptance issues of biometric authentication technology on mobile devices as experienced/brought forth by mobile users. The instrument's validity can be taken as the degree to which the instrument reveals the abstract construct being evaluated (Golafshani, 2003). Numerous factors could have an influence on the internal and external validity of the assessing instruments, for example, the survey questionnaire used to collect data regarding the acceptance of biometric authentication security technology on mobile devices.

3.9.1.1. Internal validity

Internal validity is the exact truth regarding inferences about cause-effect or causal relationship (Sedgwick, 2012). In this study, internal validity is the degree to which the factors, identified as acceptance issues for biometric authentication security technology on mobile devices by mobile users truly reflect what hinders effective acceptance and usage of this technology.

3.9.1.1.1. Threats to internal validity

The occurrence of a situation, which might not be related to the study, but can have an effect on the results of the study presents a possible threat to the internal validity of the data (Jankowski, Flannelly and Flannelly, 2018). The most significant threats to the internal validity of the current study were factors associated with the history of the participants' biometric authentication technology usage and the procedure used to select study participants. Numerous factors in this survey have been identified as biometric challenges, for instance, the lack of knowledge regarding biometric authentication technology or challenges experienced by biometric users on mobile devices.

3.9.1.2. External validity

External validity can be described as the degree to which research findings can be generalised beyond the sample that was used in the study (Sedgwick, 2012). In this study external validity was ensured.

3.9.1.2.1. Threats to external validity

In a research project the external validity can be threatened by the sampling technique chosen, the validity of the assessing instruments (survey questionnaire in this case) and the predictive value of the research instruments (Jankowski, Flannelly and Flannelly, 2018).

- Sampling techniques

The kinds of sampling techniques used have an effect on the generalisability of the study findings to the whole population, thereby posing a threat to the external validity of the findings (Jankowski, Flannelly and Flannelly, 2018). For the purpose of this study, a simple random sampling technique was used and a sample of 302 participants was obtained.

- Validity of assessing instruments

Jankowski, Flannelly and Flannelly (2018) said that a valid instrument assesses the concept in question, and it assesses it appropriately. There are three main categories of estimating the validity of the data collection instruments. These include self-evident assessment, pragmatism assessment and construct validity (Jankowski, Flannelly and Flannelly, 2018). In the current study, the validity of the assessing instrument was observed by sticking to the characteristics of all three assessments.

Self-evident assessment

Self-evident assessment refers to the degree to which the instrument assesses what it is supposed to assess, which can be categorised as face and content validity (Jankowski, Flannelly and Flannelly, 2018). In ensuring face validity the pilot study was conducted to assess the research instruments.

Content validity is the degree to which the content of the research instrument appears to comprehensively evaluate the scope it is intended to assess (Jankowski, Flannelly and Flannelly, 2018). A literature review was done on technology acceptance, biometric acceptance and mobile biometric acceptance. The information provided by the literature review assisted in setting the research questions of this study and assisted the researcher to incorporate the relevant content guiding the achievement of the study objectives.

Pragmatic assessment

Pragmatic assessments are a way of establishing validity by focusing on the practical value of the instrument through concurrent and predictive validity (Jankowski, Flannelly and Flannelly, 2018). This study used predictive validity by predicting the future changes in the key concepts, by specifying the assumptions underlying this study (found in chapter 4).

3.9.2. Reliability

Reliability is the extent to which the research instrument assesses an attribute (Golafshani, 2003). It can further be described as the degree to which independent administration of the same tool produces the same results under conditions that are comparable (Golafshani, 2003). Reliability is related to validity, which means that a tool which is not valid cannot possibly be reliable. Reliability was ensured in this study.

3.10. Pilot study

A pilot study is a small-scale preparatory study that is carried out for the purpose of evaluating duration, feasibility, cost, unfavourable events and improvement on the study design before the execution of a full-scale research project (Thabane *et al*., 2010). Thabane *et al*. (2010) said that pilot tests are usually conducted before a large-scale quantitative study in an attempt to prevent time loss and costs of an insufficiently designed project. This study is frequently conducted on participants belonging to the relevant population (Thabane *et al*., 2010).

According to Cadete (2017), a pilot study must provide an answer to an easy question such as "Can the full-scale study be carried out according to the way that it has been planned or should other elements be altered?" In order to allow readers to interpret the findings and implications correctly, a high quality report of the pilot study must be produced (Cadete, 2017). Cadete (2017) indicated why a pilot study should be conducted and the reasons are as follows:

- Process: where the feasibility of the major steps in the main study is evaluated (for example, the level of retention, rate of recruitment and criteria of eligibility).
- Resources: evaluating issues with time and equipment that might occur during the main study (for example, how long will it take for the main study to be completed; whether utilisation of some resources will be feasible or whether the forms of assessment chosen for the main study are as great as possible).
- Management: issues with data management and with participants who partook in the study (for example, whether there were issues with gathering the overall data required for future analysis; whether the gathered data are highly variable and whether the data from various institutions can be analysed altogether).

3.10.1. The pilot study in the current research

In order to reduce misunderstandings and also unclear questions a pilot study was initiated. Meriwether (2001) indicated that a pilot study helps researchers to make minor changes so as to enhance or clarify data and appropriate procedures. The list below indicates how a pilot study can help a researcher:

- Length: Ensure that the length of the questionnaire is not too long.
- Clarification: To ensure clear instructions with good layout.
- Reliability: This is the pre-testing stage in which the reliability of the questionnaire is improved.

3.10.2. The pilot study aims in the current research

The main aim of the pilot study was to test the questionnaire. This was done to reduce the imperfections (if any) and to validate the survey questions and also to check whether respondents understood the questions. Furthermore, the pilot study gave information regarding the response rate and assisted in determining the data collection method that was relevant based on the content and data procedures. Gilbert (2001) indicated that a pilot study assists researchers to ensure the acceptability of the questionnaire, design a research procedure, evaluate whether the research procedure is workable and to gather preliminary data.

3.10.3. Selection of participants for the pilot study

A sample of the chosen survey population was used to test the questionnaire and the procedures in order to ensure sufficient application of the pilot study. Tabachnick and Fidell (2005) indicated that the pilot study subjects should be around 10% of the sample size to conduct a pilot study. The questionnaire was distributed to 30 randomly selected individuals as this number was 10% of the target population which is in line with (Tabachnick and Fidell, 2005). This selection helped in producing adequate feedback regarding the questionnaire contents and procedures of the research.

The following are the main selection criteria used for the participants of the pilot study:

- Nationality: To know the nationality of the participants.
- Gender: To compare samples of females with males.

- Education: To know the level of education of the participants.
- Employment status: To know the employment status of the participants.
- Age: To know the age group category of the participants

3.10.4. Pilot study phases

The researcher conducted numerous phases in the pilot study:

- The first phase was a questionnaire drafting. All questionnaires were drafted in English because the majority of the target population would understand it in this language.
- The second phase was to ensure correspondence between the questionnaire and the study objectives as well as to ensure reasonable length of the questionnaire.

The following information was provided for statistical purposes and to ensure an adequate level of analysis:

- A covering letter was attached to introduce the study, its purpose and the significance of responding to the questionnaire in order to achieve the research objectives. Hand copies of questionnaires were given to each participant as well as soft copies for participants who needed them.

3.11. Data analysis

For the purpose of this study, data were analysed using the Statistical Package for Social Sciences (SPSS). According to Gunarto and Hary (2019), SPSS is a broadly utilised programme for statistical analysis. Furthermore, it is utilised by researchers in education, researchers in health, researchers in survey companies, researchers in marketing organisations, data miners, researchers in government etc. In analysing data for this study, a few steps were completed:

Step one: The SPSS software was used to transform the raw data into quantifiable data.

Step two: The quantified data that were obtained, was then further examined to give evidential data that would assist in the research process.

Step three: The data was entered onto a spreadsheet and coded or organised to provide a meaning (nominal, interval, ordinal or ratio).

Step four: The raw data was summarised or described to simplify the pattern identification or to visualise what was shown by the data using descriptive statistics (percentages, frequencies, means, modes etc.).

Step five: The differences and associations among two or more population samples were examined. To carry out this task the following tests were made:

- Factor analysis: The proposed model was tested to see if it was appropriate for factor analysis.
- Assumptions: The data were checked to see if it contained the outliers, and checked for normality, presupposition of linearity, homoscedasticity, validity, reliability and multicollinearity.
- Correlations: The correlation was used to describe the nature of the association among two variables by identifying whether the existing relationship was positive, strong, weak, negative or statistically significant.
- ANOVA: This analysis was performed in order to find out if the means of the variables were statistically significant and also to confirm if the differences were substantial.
- Regression: The regression helped to find out whether one variable was the determinant of another variable.

3.12. Quality criteria

This study ensured the following quality criteria:

- Internal validity: The degree to which observed effects can be attributed to the independent variable.
- External validity: The degree to which the findings can be generalised from the research sample to the population.
- Reliability: The degree to which the findings would be consistent if the research was duplicated.
- Objectivity: The degree to which individual biases are removed and value free data gathered.

3.13. Scope and limitations of the current study

The scope of this study included the following:

- South African citizens in Johannesburg (Vanderbijlpark) which will be defined as follows:

The total number of 305 participants must be provided with a survey questionnaire to answer.

- A mobile device which refers to any portable electronic device that can connect to a network such as the internet.
- Biometrics which refers to a system that is fundamentally a pattern-identification system.
- User's perceptions of acceptance of biometric authentication technology on mobile devices.

3.13.1. Limitations of the study

For this study, there are two major limitations that could be addressed in future research. These were:

- Lack of previous research studies on the topic: relevant research studies for the topic of this thesis are limited.
- Limited access to data: due to the COVID-19 pandemic in the country, the researcher had a limited access to respondents.

3.14. Ethical considerations

The participants were given a participant information sheet, which informed them of ethical considerations that the research observed as follows:

3.14.1. The right to self-determination

It is of vital importance that the participants are not forced or obliged to partake in the study as indicated in the self-determination right. Collis and Hussey (2003) indicated that if the participants refuse to partake in the study then no penalty should be enforced upon them. The researcher clearly explained the study objectives to the participants through the consent form. Furthermore, the researcher indicated before the project started that the participants were free to quit at any point without any issue. Participants were not pushed to partake in the project and consent was received from every participant before the project began.

3.14.2. Informed consent

The intention of the study was explained to the participants on the participant information sheet, and they were asked to cooperate. The study's purpose was clarified, and participants were given the option of participating or not participating in the study. The participants were told that

participation in the study was completely voluntary, and that if they decided to participate, they could withdraw at any time.

3.14.3. The right to disclosure

This principle indicates that all the aims and objectives of the study must be briefed to the potential participants in detail by the researcher. Collis and Hussey (2003) confirm that the notion of full disclosure depends on self-determination. As highlighted earlier, all the information regarding the purpose of the study was explained to the participants.

3.14.4. Privacy and confidentiality

Every person is entitled to confidentiality and privacy both on ethical grounds and in terms of the protection of their individual and sensitive data under the Data Protection Act (Collis and Hussey, 2003). The researcher ensured that participants had the freedom to decide the time, extent and situations under which they would withhold or share information.

3.15. Conclusion

Much study has been conducted on technology acceptance and adoption. This study was quantitative and conducted using a non-experimental research design. A total number of three hundred and five (305) participants were chosen to partake in this study. The participants were selected using a simple random sampling technique. The researcher ensured validity and reliability of the study and observed ethical considerations. The results of the study will be analysed using descriptive statistics and inferential statistics.

Chapter four: Developing a proposed Mobile Biometric Technology Acceptance Model (MBTAM)

4.1. Introduction

The second objective of this study was to propose a model that can be used to measure the acceptance of biometric authentication technology on mobile devices. This chapter aims to present the proposed model in order to fulfil the above mentioned objective. Furthermore, this chapter discusses how the proposed model was developed. For the development of the proposed model based on the variables in chapter 2, the Biometric User Acceptance Model by Ho, Stephens and Jamieson (2003) will be reviewed. After the review, the presentation of the proposed Mobile Biometric Technology Acceptance Model derived from Ho, Stephens and Jamieson (2003) will follow. Hypotheses for this study will then be stated after the presentation of the proposed model.

The proposed Mobile Biometric Technology Acceptance Mode (MBTAM)

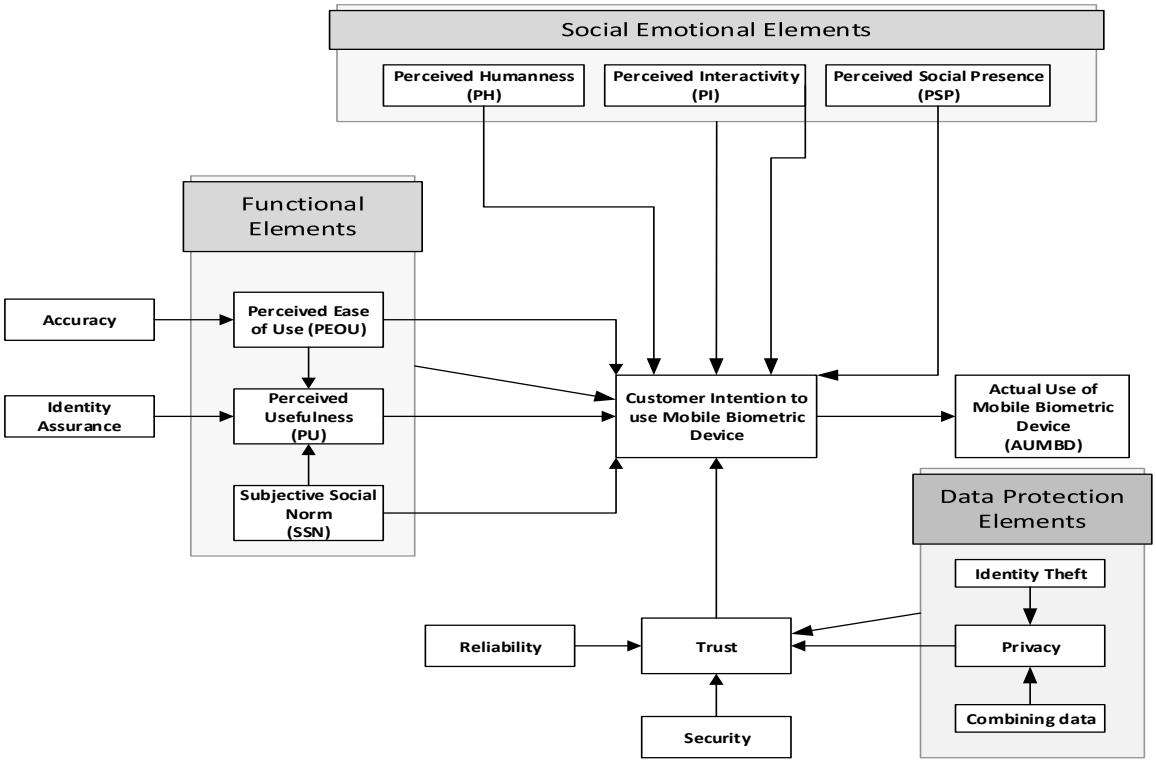


Figure 4. 1 Proposed Mobile Biometric Technology Acceptance Model for this study (Derived from Ho, Stephens and Jmieson, 2003 and Wirtz *et al.* 2020).

The technology acceptance model by Davis, Bagozzi and Warshaw (1989) gives the root for comprehending the issues regarding the acceptance of mobile biometric technology. In order for perceived ease of use and perceived usefulness to be relevant for a biometric system, their definitions must be modified (Ho, Stephens and Jamieson, 2003). Therefore, the researcher proposes that numerous contributing factors and issues related to the development of the proposed model for this study must be modified (by adding or removing). These are shown in Figure 4.1.

Perceived usefulness was defined as "the degree to which a being believes that utilising a specific framework will improve his or her work performance" (Davis, Bagozzi, and Warshaw, 1989, p. 320). According to Ho, Stephens and Jamieson (2003), perceived usefulness of a biometric verification system is not directly associated with work performance. Therefore, Ho, Stephens and Jamieson (2003) define perceived usefulness widely as the degree to which a being believes that utilising a specific biometric framework would achieve the organisation's security access requirements in a specific domain.

As per the definition of perceived usefulness provided above, the subjective norm, image, output quality and identity assurance of a biometric system are determining factors of perceived usefulness (Ho, Stephens and Jamieson, 2003). Mobile devices have ubiquitous strength because they are globally accessible (Zydney and Warner, 2016). Thus, for the purpose of this study only identity assurance and subjective norm (as subjective social norm) were considered to be the determinant of perceived usefulness since data sensitivity is independent of the technology; however future changes may be made to this model.

Security is associated with the integrity, confidentiality and availability of the data that is being processed and stored by a system (Ho, Stephens and Jamieson, 2003). In the context of biometrics, factors such as the ease with which counterfeits can be made, the probability of replay attacks, and the vulnerability to brute-force attacks all influence security (Biometrics, 2020). Furthermore, in the context of mobile devices, security is defined as measures taken to protect sensitive data stored on portable devices (Lerner, 2019). The greater the security of the system, the more the trust it will gain from users (Kyrezis and Dmitriadis, 2010).

Accuracy is defined as the degree to which the system is capable of matching a biometric sample with its pre-existing template accurately in a real world setting (Ho, Stephens and Jamieson, 2003). According to Ho, Stephens and Jamieson (2003), the accuracy of a biometric framework is dependent on its rate of errors (for example, false rejection rate, false acceptance rate and failure to enrol rate). Perhaps accuracy is the most important determinant of perceived ease of use.

The likelihood that a system would not fail to achieve its expected goals is known as its reliability (Ho, Stephens and Jamieson, 2003). Reliability of the system can determine the security of the system; however security on its own makes some contributions to reliability (Burtescu, 2010). For a biometric system it is going to be even more successful and important because of its use and context of security (Biometrics, 2020).

Ho, Stephens and Jamieson (2003) said that the TAM description of perceived ease of use does not need to be modified and it suits the context of a biometric system in the way it was defined by Davis, Bagozzi and Warshaw (1989). They defined it as "the degree to which a being believes that utilising a specific framework would be free of effort".

According to Ho, Stephens and Jamieson (2003), a biometric system intrinsically varies according to the individual data it uses. This results in information privacy which is defined as "the ability of the person to individually manage information regarding one's self" (Petters, 2020) turning out to be more important. One of the usual privacy issues indicated by (Biometrics, 2020) includes:

- Combining data: Concern with the possibility that data from databases that are disparate might be merged into larger databases.

Individual privacy turns out to be one of the main concerns beings have when taking biometrics into consideration than traditional authentication techniques (Ho, Stephens and Jamieson, 2003). Such worry is quite justified taking into consideration the highly individual information involved. Identity theft is promoted to a new level if a biometric indication is in some way counterfeited (Ho, Stephens and Jamieson, 2003). Thus, privacy shapes people's trust in using mobile biometric devices (Kyrezis, 2010).

To add social elements to the proposed model, Wirtz *et al*. (2020) indicated that all social elements (specifically, perceived humanness, perceived interactivity and perceived social presence) are important determinants of users' intention to use an innovation. Moreover, functional elements (perceived ease of use, perceived usefulness and subjective social norm) are also important as they are great determinants of a user's intention to use a particular technology (Wirtz, 2020).

4.2. Hypotheses

Based on the results obtained above, this study will test the following hypotheses:

H_{01}: Perceived humanness has a positive influence on intention to use.

H_{02}: Perceived interactivity has a positive influence on intention to use.

H_{03}: Perceived social presence has a positive influence on intention to use.

H_{04}: Perceived ease of use has a positive influence on intention to use.

H_{05}: Perceived usefulness has a positive influence on intention to use.

H_{06}: Subjective social norm has a positive influence on intention to use.

H_{07}: Trust has a positive influence on intention to use.

H_{08}: Perceived ease of use has a positive influence on perceived usefulness.

H_{09}: Subjective social norm has a positive influence on perceived usefulness.

H_{10}: Accuracy has a positive influence on perceived ease of use.

H_{11}: Identity assurance does not have an influence on perceived usefulness.

H_{12}: Intention to use has a positive influence on actual use.

H_{13}: Reliability has a positive influence on trust.

H_{14}: Security has a positive influence on trust.

H_{15}: Privacy has a positive influence on trust.

H_{16}: Identity theft has a positive influence on privacy.

H_{17}: Combining data has a positive influence on privacy.

H_{18}: Functional elements have a positive influence on intention to use.

H_{19}: Social elements have a positive influence on intention to use.

H_{20}: Data protection elements have a positive influence on trust.

4.3. The presentation of the proposed model

Figure 4.2 indicate the proposed Mobile Biometric Technology Acceptance Model

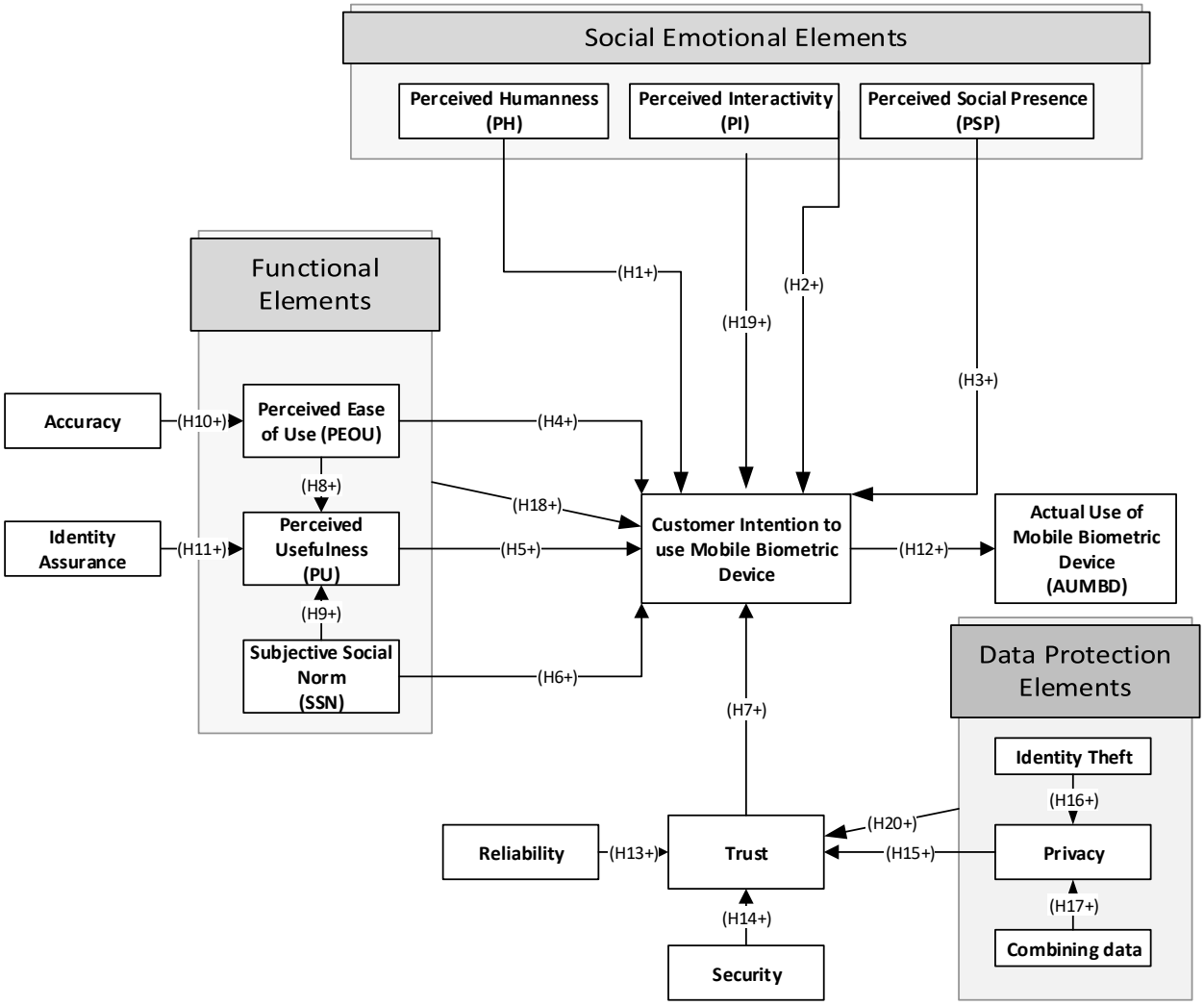


Figure 4. 2 Proposed Mobile Biometric Technology Acceptance Model for investigation (Derived from Ho, Stephens and Jmieson, 2003 and Wirtz *et al.* 2020)

4.4. Conclusion

In this chapter, the development of the proposed model and hypotheses were stated. The next chapter will give the detailed information regarding the research methodology and all processes that were used to develop the proposed model.

Chapter five: Descriptive analysis

5.1. Introduction

This chapter presents a descriptive analysis of the data obtained through data collection instruments. The overarching goal of this study was to determine how biometric authentication technology on mobile devices was perceived. The questionnaire used in this quantitative study was carefully analysed to ensure that the data gathered was presented clearly with the aid of tables, percentages and charts, where possible.

5.2. Sample results

Of the original sample size of three hundred and five (305) participants, only three hundred and two (302) responded. The remaining three (3) participants had to engage in another survey questionnaire and had other commitments which were the reasons they did not manage to take part in this study. This left three hundred and two (302) participants.

5.2.1. Response rate

A total number of three hundred and five (305) survey questionnaires were distributed. However, a total number of three hundred and two (302) responses were received. This is a response rate of 98%.

5.2.2. Demographic characteristics

This section outlines the demographic characteristics of the respondents which include gender of the participants, age, employment status, level of study of the participants (only applicable to students), question on whether a participant owned a mobile device or not, question that aimed to find out if the participant had knowledge of biometric security authentication technology, question that aimed to find out if a participant would prefer to use mobile biometric device in

future and question that aimed to find out if a participant had knowledge of the internet and scams.

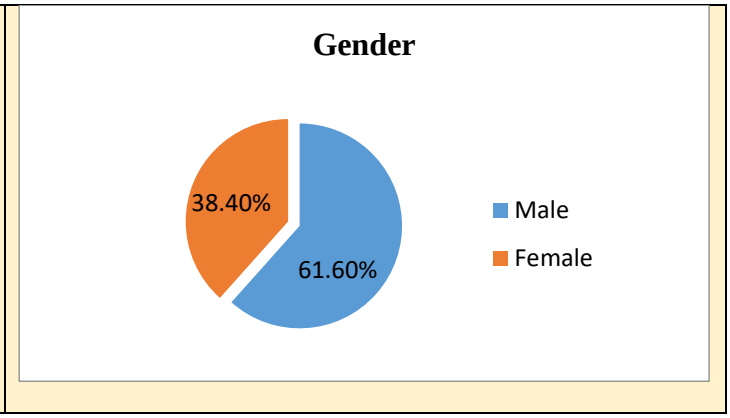
5.2.2.1. Gender

The gender of the respondents was based on two (2) categories (Table 5.1):

- The first group of respondents was classified as “Male” with (61.6%).
- The second group of respondents was classified as “Female” with (38.4%).

Table 5.1 Gender

		Frequency	Percent
Valid	Male	186	61.6%
	Female	116	38.4%
	Total	302	100.0%



5.2.2.2. Age

The age of the respondents was based on six (6) categories (Table 5.2):

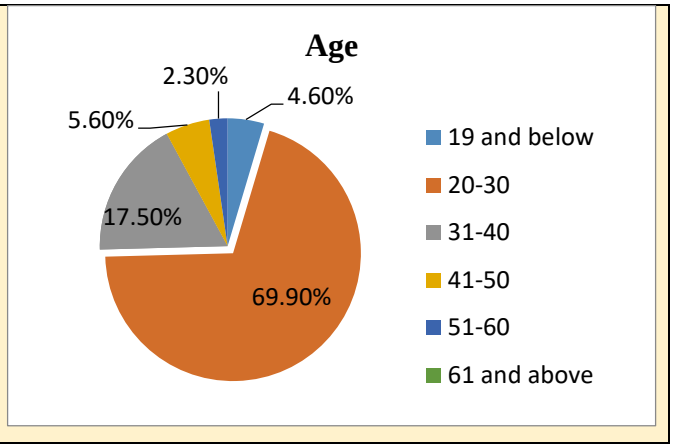
- The first group of respondents came from the age group that was “19 and below” with 4.6%.
- The second group of respondents came from the age group that was between 20 and 30 with 69.9%.
- The third group of respondents came from the age group that was between 31 and 40 with 17.5%.
- The fourth group of respondents came from the age group that was between 41 and 50 with 5.6%.
- The fifth group of respondents came from the age group that was between 51 and 60 with 2.3%.

- The last age group category was “60 and above” which had zero (0) respondents.

These findings show that the largest group of respondents came from the age group that was classified as “20-30” with 69.9%. Moreover the smallest group of respondents came from the age group that was classified as “61 and above” which had 0%.

Table 5. 2 Age

		Frequency	Percent
Valid	19 and below	14	4.6%
	20-30	211	69.9%
	31-40	53	17.5%
	41-50	17	5.6%
	51-60	7	2.3%
	61 and above	0	0%
	Total	302	100.0%



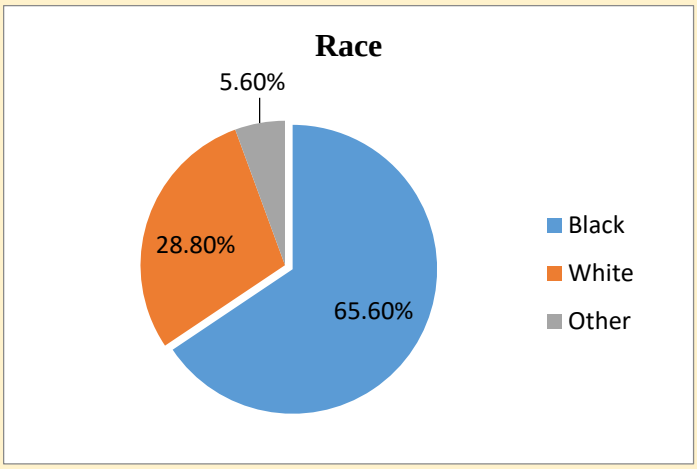
5.2.2.3. Race

The race of the respondents was based on three (3) categories (Table 5.3):

- The largest group of respondents came from the race that was classified as “Black” with 65.6%.
- The second largest group of respondents came from the race that was classified as “White” with 28.8%.
- Lastly, the smallest group of respondents came from the race that was classified as “Other” with 5.6%.

Table 5.3 Race

		Frequency	Percent
Valid	Black	198	65.6%
	White	87	28.8%
	Other	17	5.6%
	Total	302	100.0%



5.2.2.4. Employment status

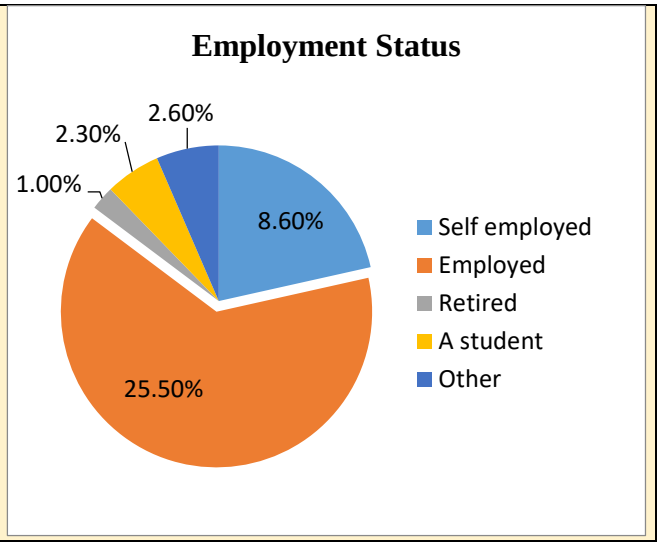
The employment status of the participants was based on five (5) categories (Table 5.4):

- The first group of the respondents came from the employment status that was classified as “Self-employed” with 8.6%.
- The second group of the respondents came from the employment status that was classified as “Employed” with 25.5%.
- The third group of the respondents came from the employment status that was classified as “Retired” with 1.0%.
- The fourth group of the respondents came from the employment status that was classified as “A student” with 62.3%.
- The last group of the respondents came from the employment status that was classified as “Other” with 2.6%.

These findings show that the largest group of respondents came from the employment status that was classified as “A student” with 62.3% and the smallest group of respondents came from the employment status that was classified as “Retired” with 1.0%.

Table 5.4 Employment status

		Frequency	Percent
Valid	Self employed	26	8.6%
	Employed	77	25.5%
	Retired	3	1.0%
	A student	188	62.3%
	Other	8	2.6%
	Total	302	100.0%



5.2.2.5. Level of study (Only applicable to students)

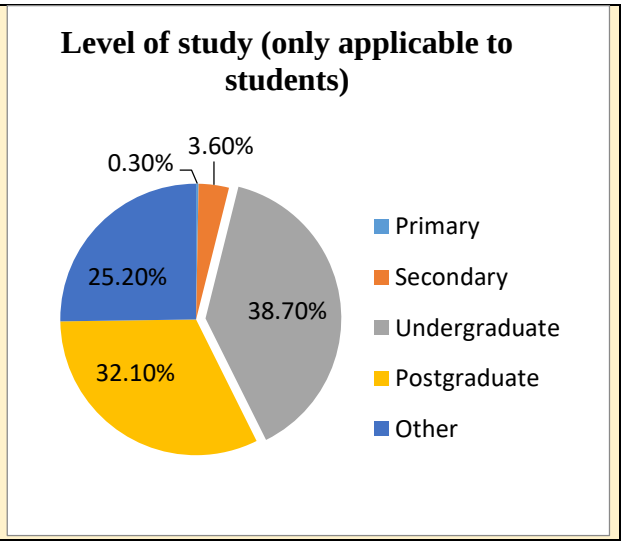
The level of study of the participants was based on five (5) categories (Table 5.5):

- The first group of the respondents came from the level of study that was classified as "Primary" with .3%.
- The Second group of the respondents came from the level of study that was classified as "Secondary" with 3.6%.
- The third group of the respondents came from the level of study that was classified as "Undergraduate" with 38.7%.
- The fourth group of the respondents came from the level of study that was classified as "Postgraduate" with 32.1%.
- The last group of the respondents came from the level of study that was classified as "Other" with 25.2%.

These findings show that the largest group of respondents came from the level of study that was classified as "Undergraduate" with 38.7% and the smallest group of respondents came from the level of study that was classified as "Primary" with .3%.

Table 5.5 Level of study (only applicable to students)

		Frequency	Percent
Valid	Primary	1	.3%
	Secondary	11	3.6%
	Undergraduate	117	38.7%
	Postgraduate	97	32.1%
	Other	76	25.2%
	Total	302	100.0%



5.2.3. Descriptive analysis results

In order to find out if respondents were currently owning mobile devices or would prefer to use mobile biometric devices in future and to find out whether respondents had knowledge of biometric authentication security technology or had accessed the internet using mobile biometric devices, respondents were asked questions with “Yes”, “No”, “Not sure” or “Owned it before” categories (Table 5.6).

It was found that the largest group of two hundred and ninety-four (294) respondents owns mobile devices (97.4%) and the second largest group of five (5) respondents owned mobile devices before (1.7%). However, only three (3) respondents did not own mobile devices (1.0%). Furthermore, as the questionnaire was trying to determine the respondents’ experience of biometric authentication security technology, it was found that the largest group of two hundred and fifteen (215) respondents used biometric authentication security technology before (71.2%). It was only a small group of eighty seven (87) respondents which has never used biometric authentication security technology before (28.8%).

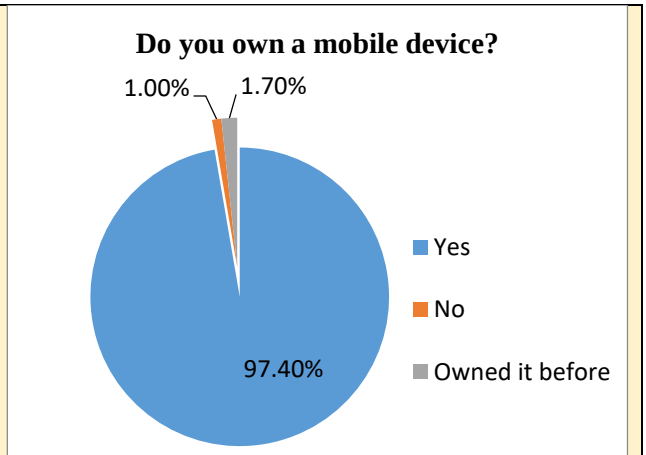
The questionnaire on whether respondents would prefer to use mobile biometric devices in the future was distributed. It was found that the largest group of two hundred and fifty-six (256)

respondents would prefer to use mobile biometric devices (84.8%). However, thirty one (31) respondents are not sure if they would prefer to use mobile biometric devices (10.3%) and fifteen (15) respondents replied that they do not prefer to use mobile biometric devices (5.0%). The study tried to determine if respondents accessed the internet using mobile biometric devices and it was found that the largest group of one hundred and sixty-one (161) respondents did not access internet using a mobile biometric device (53.3%). However, one hundred and forty-one (141) respondents accessed the internet using mobile biometrics (46.7%).

Table 5. 6 Usage and intent to use mobile biometric device

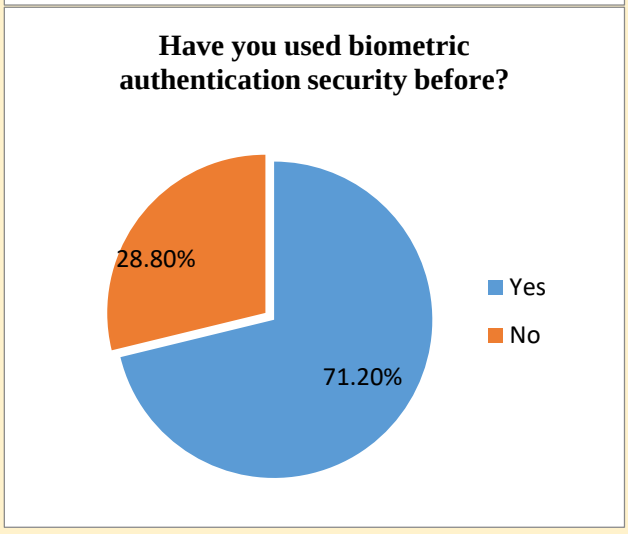
Do you own a mobile device?

		Frequency	Percent
Valid	Yes	294	97.4%
	No	3	1.0%
	Owned it before	5	1.7%
	Total	302	100.0%



Have you used biometric authentication security before?

		Frequency	Percent
Valid	Yes	215	71.2%
	No	87	28.8%
	Total	302	100.0%



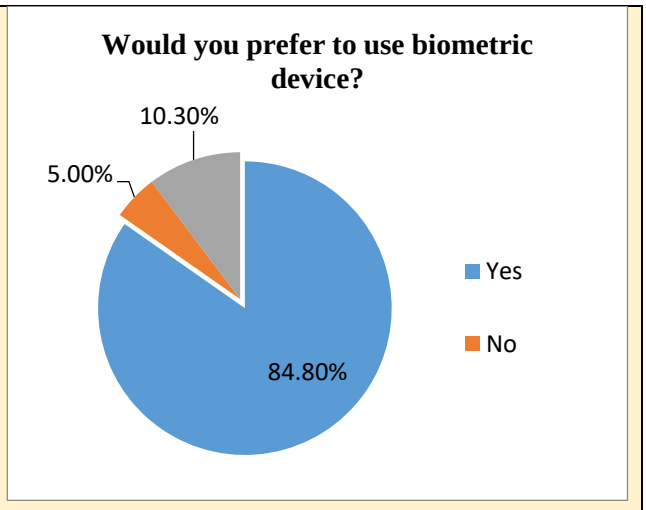
Would you prefer to use mobile biometric device?

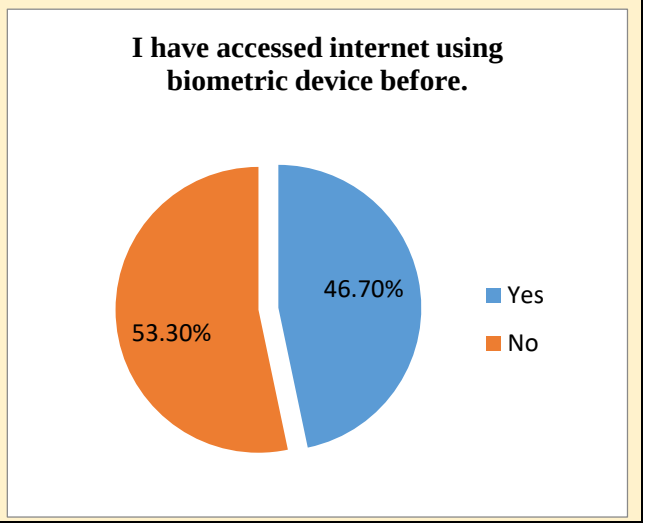
		Frequency	Percent
Valid	Yes	256	84.8%

	No	15	5.0%
	Not sure	31	10.3%
	Total	302	100.0%

I have accessed the internet using a mobile biometric device before.

		Frequency	Percent
Valid	Yes	141	46.7%
	No	161	53.3%
	Total	302	100.0%





5.3. Reliability analysis

5.3.1. Items reliability analysis

In this section, all research model variables have been assessed for reliability, convergent and discriminate validity. Concerning reliability test, Cronbach's Alpha was used to determine the internal consistency of each variable, ensuring that all of the scale's elements were properly interrelated.

Cronbach's Alpha was chosen for this purpose since it is regularly adopted in science studies and it is known as a measure of reliability (Taber, 2017). According to Abraham and Barker (2014) reliability estimates of 0.70 can be considered for adequate basic research, whereas other researchers believe that a high degree of reliability could result in a coefficient value of 0.60 to

0.70. (Griethuijsen *et al*., 2014). Taber (2017) said that values were defined as excellent if they have Cronbach's alpha of 0.93 to 0.94, strong (0.91 to 0.93), reliable (0.84 to 0.90), robust (0.81), fairly high (0.76 to 0.95), good (0.71-0.91) and low (0.11).

In this study, the reliability analysis of all variables indicates that the Cronbach's Alpha value was .811, as indicated in Table 5.7

Table 5. 7 reliability statistics

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	No. of Items
.811	.824	16

The Chronbach's Alpha was used to measure the internal consistency and a scale of reliability for variables in the model of this study. Table 5.7 indicates that the internal consistency amongst the variables was robust and greater than the recommended minimum.

5.3.2. Items validity

Item validity is a quality of estimation concerned with the degree that a test estimates what we really wish to measure (Gliem and Gliem, 2003). For the purpose of this study, Cronbach's Alpha if the item deleted column was carefully considered when performing the item validity test. This is the most important column in the table because it represents the scale's Cronbach's alpha reliability coefficient for internal consistency if the individual item is removed from the scale (Gliem and Gliem, 2003). This value is then compared to the Alpha coefficient value at the bottom of the table to see if one wants to delete or keep the item. According to Gliem and Gliem (2003) an item can be deleted only if its removal would increase the Cronbach's Alpha coefficient value and such items are considered invalid items and the item can be kept if its removal will decrease the Cronbach's Alpha coefficient value and such items are considered valid items.

A reliability analysis was performed on the sum of the questionnaire for each variable as indicated in Table 4.8. Cronbach's alpha showed the questionnaire to reach acceptable reliability

(α = .775). All items appeared to be worthy of being kept since their removal might result to the decrease of the overall Cronbach's Alpha (Table 5.9). The results highlighted the satisfactory level of construct validity and internal consistency of the items.

Table 5. 8 reliability statistics

Cronbach's Alpha	N of Items
.775	16

Table 5. 9 Item-total statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Perceived Usefulness	83.1457	326.517	.392	.762
Perceived Ease of Use	83.1954	327.314	.397	.761
Social Subjective Norm	80.4106	326.276	.311	.774
Trust	80.7914	299.202	.381	.773
Perceived Humanness	84.4470	330.401	.503	.753
Perceived Interactivity	84.8841	339.485	.453	.758
Perceived Social Presence	83.6689	314.375	.606	.743
Actual Use	83.0960	331.516	.328	.768
Accuracy	86.4007	340.008	.537	.755
Identity Theft	86.1060	362.680	.321	.773
Reliability	88.5033	357.174	.463	.765
Privacy	86.3742	350.860	.383	.764
Security	86.3709	347.855	.391	.763
Identity Assurance	86.4536	338.740	.568	.754
Combining Data	88.5596	364.506	.322	.771

Intention to Use	87.0795	339.907	.593	.754

5.4. Factor analysis

Factor analysis is known as a broad term that incorporates a range of statistical techniques that make it possible to predict the overall population. This prediction is achieved by a variety of observed variables and association amongst them (Akyuz, 2018). According to Pett, Lackey and Sullivan (2003), factor analysis is part of the General Linear Model (GLM) and this method also assumes numerous assumptions: there is a linear relationship, there is no multicollinearity, it includes relevant variables into analysis and there is a true correlation amongst variables and factors.

Exploratory factor analysis is one of the most important data analysis methods (Zeynivandnezhad, Rashed and Kanooini, 2019). According to Pallant (2011) this method assumes that any indicator or variable may be associated with any factor. For the purpose of this study, the data set was subjected to exploratory factor analysis in order to classify and isolate the large number of variables into a smaller number of factors. This technique was chosen for this study because of its capability to reduce the number of variables and evaluate the validity of a scale, test or instrument. Furthermore, Exploratory factor analysis can be easily interpreted and address multicollinearity (Matsunaga, 2010).

According to Pallant (2011), the following steps are involved in factor analysis:

- **Assessment of the Suitability of data**

This assessment incorporates two factors: sample size and the strength of the association amongst the variables. In line with Saunders, Lewis and Thornhill (2007), the minimum sample could be 30. Furthermore, for executing factor analysis, the minimum sample size, according to Tabachnick and Fidell (2007), should be at least 100. Nevertheless, the sample size for this analysis was 305, which is higher than the recommended number and helps to strengthen the generalisation of the findings.

- **Factor Extraction**

In this stage, the factors that can be utilised to best signify the interrelations amongst items are involved (Pallant, 2011). Even if there are various forms of extraction techniques that can be used, for example, factor component, principal component etc. The most regularly used technique is a principal component (Pallant, 2011).

Kaizer's criterion and Scree Plot were suggested by Pallant (2011) as techniques that can be used to determine the number of factors to retain. According to this test, Kaiser's criterion is known as Eigenvalue.

- **Data rotation**

There are two key approaches that can be utilised for rotation. These incorporate orthogonal and oblique (Pallant, 2011). Orthogonal approach states that the underlying constructs are not correlated and is mostly used to maximize the variance of factor loadings by making high loading the highest and low ones the lowest for each other (Tabachnick and Fidell, 2007). Thus, Variables with a loading greater than.3 will be included, while those with a lower loading will be excluded (Pallant, 2011). The oblique method presumes that underlying constructs are related (Tabachnick and Fidell, 2007).

Many studies prefer to use the orthogonal approach because it is easy to be interpreted (Tabachnick and Fidell, 2007). It is suitable also for this study and for the purpose of this study; the Varimax rotation (orthogonal) was used. George and Mallery (2006) said that factor loadings indicate the strength of the association amongst the variables and factors, which differs between -1.0 and +1.0.

Factor loadings greater than 0.4 (which is the loading variables for cut-off limit) are considered to be acceptable and indicate the excellent face validity while factor loadings less than 0.4 shows that the variable should be eliminated from the analysis (Samuels, 2016). Other researchers (George and Mallery, 2006) recommend that the loading factor should exceed 0.5 while others (Knafl and Grey, 2007) recommend that the loading should exceed 0.3. The loading factor will be greater than 0.4 for the purposes of this study.

5.4.1. Factor analysis results

In executing the factor analysis, there are three steps that should be performed which incorporate determining the factors, interpreting the factors and selecting the final factor solution (Samuels, 2016).

- **Data suitability for the Factor Analytic Techniques**

Firstly, the data were tested for its suitability for factor analysis. This was achieved using the Kaiser-Meyer-Oklin (KMO) value. Reba, Birhane and Gutema (2019) said that KMO measure that exceeds 0.5 is adequate for valid factor analysis, a value of 0.70 is taken as "reasonable" and a value of 0.80 is taken as "good" and values that exceed 0.9 are excellent.

The primary solution for factor analysis of this study revealed a KMO value of 0.800, which is good according to Reba, Birhane and Gutema (2019) and is higher than the recommended value of 0.6 (Pallant, 2011). The factorability of the correlation matrix was confirmed by the Bartlett Test of Sphericity ($p<0.001$), as shown in Table 5.10. These two findings showed that the data are suitable for factor analysis.

Table 5. 10 KMO and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.800
Bartlett's Test of Sphericity	Approx. Chi-Square	1568.696
	Df	120
	Sig.	.000

- **Factor extraction**

Factor extraction is the method of determining the factors that can be used for further analysis after the data has been validated to be appropriate for factor analysis. Table 4.9 indicates the eigenvalues related to factor prior extraction. In general, the eigenvalues related to factor analysis indicate the variance described by that specific component of linear. The eigenvalue is shown in the table as a percentage of variance described (e.g., Factor 1 describes 29.222% of

total variance). The results of extraction yield 12 factors that may be used to assess the correct number of factors to explore further. The missing values in Table 5.11 indicate that the factors were not extracted.

Table 5. 11 Total variance explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4.675	29.222	29.222	4.675	29.222	29.222
2	2.897	6.011	34.872	2.897	6.011	34.872
3	1.932	5.160	41.297	1.932	5.160	41.297
4	1.875	5.075	50.072	1.875	5.075	50.072
5	1.826	4.775	52.406	1.826	4.775	52.406
6	1.811	4.160	54.938	1.811	4.160	54.938
7	1.724	4.053	56.859	1.724	4.053	56.859
8	1.712	3.038	57.642	1.712	3.038	57.642
9	1.422	3.033	59.611	1.422	3.033	59.611
10	1.272	3.029	60.640	1.272	3.029	60.40
11	1.243	3.015	61.247	1.243	3.015	61.247
12	1.226	2.918	63.558	1.226	2.918	63.558
13	1.179	2.807	66.365	1.179	2.807	66.365
14	1.075	2.559	68.942	1.075	2.559	68.924
15	.397	2.484	94.459			
16	.290	1.813	98.307			

- **The number of factors**

There are various methods that assist in determining the number of factors chosen, however, the latent root standard is the commonly used (Barrios, 2019). The scree plot was used in this study to demonstrate the amount of factors that should be allocated for factor loading. (Figure 5.1 below).

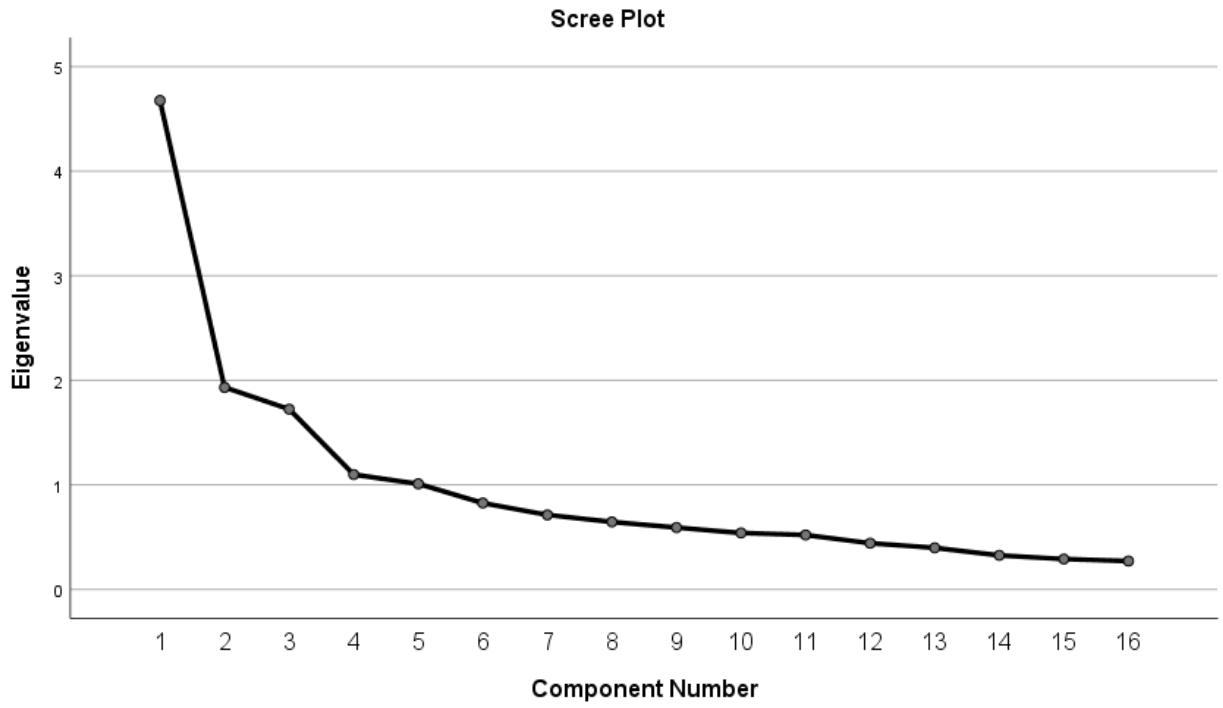


Figure 5. 1 Scree plot

- **Data rotation**

The component numbers have been recognized and now what follows is to define the pattern loadings for any interpretation. It was mentioned earlier that there are two main recognized approaches used for rotation (orthogonal and oblique) and for the purpose of this study, the varimax rotation, which is known as orthogonal was executed because it can be easily interpreted.

In executing the exploratory factor analysis test, item loadings in excess of 0.40 were retained, in agreement with the recommendations of Hair, Hult, Ringle and Sarstedt (2014), who also

recognized that item loadings are considered to be acceptable and indicate the excellent face validity with factor loadings that are greater than 0.40. The cut-off point for interpretation in this study is all loadings of .40 or above.

There are variables that do not load in any factor in some cases and the researcher has two options for those variables: The first option is to interpret the solution as it is and ignore those variables, or secondly, the researcher can exclude those variables. However, Hair, Ringle and Sarstedt (2014) maintained that ignoring the variables should be based on how much those variables contribute to the research objectives.

5.5. Conclusion

After the data collection process, this chapter introduced descriptive data analysis for demographic variables. In general, this chapter contributes in defining the relationship amongst the population and its sample, defining the characteristics of the respondents (i.e. gender, education, age, etc) that both the study and the population share. The first section started by highlighting the demographic factors in frequency tables and the second section highlighted factor analysis, both using SPSS. In the next chapter multiple regression and simple linear regression analysis will be employed in order to determine the correlation relationship amongst the model variables, test the relationship amongst the model variables and the acceptance for both, and test the model fit.

Chapter six: Data analysis

Results of multiple regression analysis

6.1. Introduction

Chapter five discussed the analysis of demographic characteristics of the respondents. However, this chapter tries to discuss the correlation association amongst the independent and dependent variables that are incorporated in this study. The null value of the initial hypothesis of this study is observed in this section. Furthermore, this chapter attempts to demonstrate the outcomes of the hypothesis testing with regard to the acceptance of mobile biometric devices. This will be achieved by carrying out multiple regression analysis. The main aim of this chapter is to answer the following research question:

- How to measure the effect of every variable of the model in the acceptance of biometric authentication technology on mobile devices?

This research question will be answered by carrying out the following research objective

- To measure the effect of every variable of the model in the acceptance of biometric authentication technology on mobile devices.

6.2. Results analysis

For the purpose of this study, a Pearson's Correlation was chosen to demonstrate the association among variables. According to Sedgwick (2016), Pearson's correlation measures the strength of the linear relationship among variables. Lastly, regression analysis was chosen as the technique for data analysis.

Regression analysis is a statistical technique for predicting the association among variables which have reason and result relation (Uyanik and Guler, 2013). In this study, regression analysis was chosen for its capability and suitability for hypothesis testing and evaluating how independent variables can be used to estimate a dependent variable. Furthermore, previous studies such as Moon and Kim (2001) and Chesney (2006) also applied this technique for data analysis and it was proven suitable. According to Chesney (2006), using regression analysis is

proper since it has been utilised in past TAM and extension studies to evaluate the association between model variables. For this reason, it has been applied in this research.

In regression analysis, the F-significant test's value should be less than 0.05, suggesting a significant association between dependent and independent variables. (Uyanik and Guler, 2013). A significant value between .05 and .10 shows a weak significant association (Uyanik and Guler, 2013). When the P-value exceeds .10, it indicates that the association is not statistically significant. The R squared value is used to determine how much of the variance in the dependent variable is explained by each factor in each model. The adjusted R squared indicates the model's adequacy in fitting the sample population (Uyanik and Guler, 2013).

6.2.1. Correlation analysis

The correlation coefficient offers the association among variables and it assists in showing the direction and strength of any correlation (Schumacker and Loxam, 2004). For these reasons, it shows only the existing association among variables and not their causality.

Table 6. 1 Correlations between PU, PEOU, SSN, Trust, PH, PI, PSP and Intention to Use

		PU	PEOU	SSN	Trust	PH	PI	PSP
Intention to Use	Pearson Correlation	.664**	.680**	.607**	.679**	.669**	.684**	.686**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000
	N	302	302	302	302	302	302	302

**.Correlation is significant at the 0.01 level1 (2-tailed).

*. Correlation is significant at the 0.05 level1 (2-tailed).

The results indicate that the Pearson's Correlation value of all variables is between 0.6 and 0.8, which indicate that there is a strong positive relationship between Intention to Use and other model variables (PU, PEOU, SSN, Trust, PH, PI and PSP).

Table 6. 2 Correlations between Reliability, Security, Privacy and Trust

		Reliability	Security	Privacy	Trust
Trust	Pearson Correlation	.490**	.121*	.210**	1
	Sig. (2-tailed)	.000	.035	.000	
	N	302	302	302	302

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

The results indicate the following:

- The Pearson's Correlation value between Reliability and Trust is between 0.4 and 0.6, which indicates that there is a moderate positive relationship between these variables.
- The Pearson's Correlation value between Security and Trust is between 0.0 and 0.2, which indicates that there is a very weak positive relationship between these variables.
- The Pearson's Correlation value between Privacy and Trust is between 0.2 and 0.4, which indicates that there is a weak positive relationship between these variables

Table 6. 3 Correlations between AUMBD and Intention to Use

		Actual Use	Intention to Use
Intention to Use	Pearson Correlation	.477**	1
	Sig. (2-tailed)	.002	
	N	302	302

**. Correlation is significant at the 0.01 level (2-tailed).

The results indicate that the Pearson's Correlation value of the two variables is between 0.4 and 0.6, which indicate that there is a moderate positive relationship between Intention to Use and the Actual Use of Mobile Biometric Devices (AUMBD).

Table 6. 4 Correlations between Identity theft, Combining data and Privacy

		Identity theft	Combining data	Privacy
Privacy	Pearson Correlation	.338**	.139*	1
	Sig. (2-tailed)	.000	.016	
	N	302	302	302

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

The results indicate the following:

- The Pearson's Correlation value between Identity theft and Privacy is between 0.2 and 0.4, which indicates that there is a weak positive relationship between these variables.
- The Pearson's Correlation value between Combining data and Privacy is between 0.0 and 0.2, which indicates that there is a very weak positive relationship between these variables.

Table 6. 5 Correlations between Identity theft, Combining data and Privacy

		Accuracy	PEOU
PEOU	Pearson Correlation	.102	1
	Sig. (2-tailed)	.076	
	N	302	302

**. Correlation is significant at the 0.01 level (2-tailed).

The results indicate that the Pearson's Correlation value between Accuracy and PEOU is between 0.0 and 0.2, which indicates that there is a very weak positive relationship between these variables.

Table 6. 6 Correlations between Identity assurance and PU

		Identity assurance	PU
PU	Pearson Correlation	.155**	1
	Sig. (2-tailed)	.007	
	N	302	302

**. Correlation is significant at the 0.01 level (2-tailed).

The results indicate that the Pearson's Correlation value between Identity assurance and PU is between 0.0 and 0.2, which indicates that there is a very weak positive relationship between these variables.

Table 6. 7 Correlations between PEOU, SSN and PU

		PEOU	SSN	PU
PU	Pearson Correlation	.611**	.282**	1
	Sig. (2-tailed)	.000	.000	
	N	302	302	302

**. Correlation is significant at the 0.01 level (2-tailed).

The results indicate the following:

- The Pearson's Correlation value between PEOU and PU is between 0.6 and 0.8, which indicates that there is a strong positive relationship between these variables.
- The Pearson's Correlation value between SSN and PU is between 0.2 and 0.4, which indicates that there is a weak positive relationship between these variables.

6.2.2. Regression analysis

6.2.2.1. Testing the assumptions of multiple regression

Multiple regression analysis is a statistical technique that is used to investigate the associations amongst single dependent and multiple independent variables (Hair *et al*., 2014). According to Hair *et al*. (2014), multiple regressions are useful when employing a number of independent variables to anticipate single dependent values when they have been selected by a researcher.

For the purpose of this study, it has been predicted that there are three notable regression analyses that need to be taken into consideration for error checking in the extant data and weather data is appropriate for use in regression models. These three types of regression analyses as indicated by Hair *et al.* (2014) include; data normality, phenomenon linearity and homoscedasticity. The following section discusses the assumptions made for the purpose of this study in more details.

- **Normality**

During the regression analysis process, the assumption is made that all research variables are normally distributed. If data that do not follow the parameters of normal distribution exists, or is, for another reason, skewed, then this lack indicates that there is significant distortion in both associations and tests of the significance. De Vaus (2002) said that the effect on the outcome of analysis of normal distribution trends is limited when sample size is sufficiently large. However, Hair *et al*. (2014) indicated that when samples are above one hundred they are likely to be an accurate reflection of behaviours and trends in large groups.

The work performed for this study was evaluated as mentioned above and the normality data were found to be distributed as indicated in Figure 5.1. This indicates a level of close to normality. The diagram in Figure 6.2 shows the normal probability plot, where the observed residuals are roughly distributed.

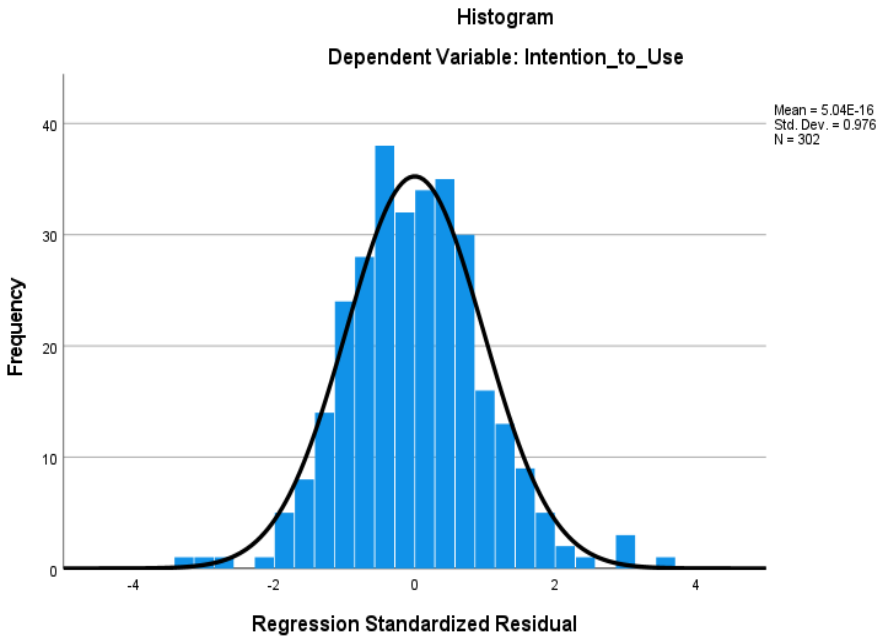


Figure 6. 1 Distribution of the data

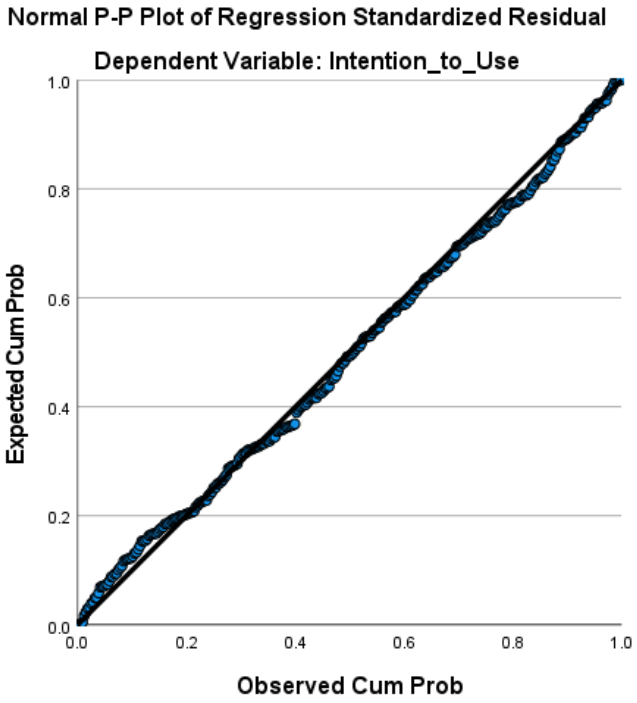


Figure 6. 2 The Normal Probability plot

Table 6. 8 Residual statistics

Residuals Statistics[a]					
	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	.5627	4.1832	1.7765	.61347	302
Std. Predicted Value	-1.978	3.923	.000	1.000	302
Standard Error of Predicted Value	.047	.241	.114	.041	302
Adjusted Predicted Value	.5425	4.2005	1.7808	.61642	302
Residual	-1.74167	1.87874	.00000	.53260	302
Std. Residual	-3.193	3.444	.000	.976	302
Stud. Residual	-3.416	3.532	-.004	1.011	302
Deleted Residual	-1.99327	1.97584	-.00430	.57115	302
Stud. Deleted Residual	-3.482	3.605	-.004	1.016	302
Mahal. Distance	1.211	57.658	13.954	11.174	302
Cook's Distance	.000	.141	.005	.015	302
Centered Leverage Value	.004	.192	.046	.037	302

a. Dependent Variable: Intention to Use

Table 5.8 indicates where standardized residual are within the range of $3 \leq -3$, which in a typical distribution sample, would expect only one per exclusion (Pallant, 2011). Furthermore, the table indicates if the unanticipated influence of the outliers on the results as a whole exists or not. One factor that has more potential to influence the model with any degree of significance is the value of Cook's distance. Tabachinck and Fidell (2007) indicate that this value should be less than one, if the value is greater than one, there is more room for significant influence on the model.

- **Linearity**

It is assumed that if the association between two variables (independent and dependent) is linear, then it follows that the results of the regression analysis will be precise. Pedhazur (2016) suggests that to detect the degree of linearity, there should be an examination of the residual plots' standardised residuals, when expressed as a function of standardised predicted value. It has

been assumed that linearity is achieved if residuals are spread according to chance and at the same time evenly through the plot of the scatter graph. The evidence produced as illustrated in the graph above (Figure 5.2) tends to suggest that the dependent variables do not defy presupposition of linearity.

- **Homoscedasticity**

It is also assumed that if the variance in error formation is equal at all levels of the independent variable, then it can be claimed that there is evidence of homoscedasticity. If homoscedasticity is discovered, there is the possibility of serious distortion and so could challenge the analysis (De Vaus, 2002). Inspection for the purposes of discovering homoscedasticity is carried out through a process of visual examination on the residual plots of real standardised values (De Vaus, 2002). This is incorporated in the regression analysis done in SPSS. The scatter graph (Figure 5.2) demonstrates that there is no presence of homoscedasticity indicated in this case.

- **Multicollinearity**

Multicollinearity arises when at least two highly correlated predictors are evaluated spontaneously in a regression model (Vatcheva, Lee, McCormick and Rahbar, 2016). The adverse impact of multicollinearity in regression analysis is well noticed and more attention to its effect is documented (Vatcheva, Lee, McCormick and Rahbar, 2016). De Vaus (2002) indicated that the evaluation of multicollinearity is well expressed by reference to both the Variable Inflation Factor (VIF) and the Tolerance Value (TV). Moreover, Kolacz (2002) indicated that a satisfactory value of TV is ≥ 0.1 where the VIF value is under 10. Table 5.9 illustrates the values of VIF and TV for the data. The results indicate that the TV values of all variables are greater than 0.1 (>0.1), and VIF values of all variables are less than 10 (<10), which implies that they are acceptable in their range of values.

Table 6. 9 Collinearity statistics

Model		Collinearity Statistics	
		Tolerance	VIF
1	(Constant)		
	PU	.564	1.773
	PEOU	.578	1.729
	SSN	.890	1.124
	Trust	.562	1.781
	PH	.630	1.588
	PI	.690	1.450
	PSP	.585	1.710
	Accuracy	.588	1.700
	Identity theft	.722	1.385
	Reliability	.532	1.880
	Privacy	.566	1.766
	Security	.510	1.962
	Identity assurance	.605	1.654
	Combining data	.638	1.566

a. Dependent Variable: Intention to Use

6.2.3. Analysis of the regression models

The hypothesis of this study is looking to ascertain the effects of the independent variables. A number of regression analysis experiments were undergone to verify the veracity of the accumulated data. Linear regression analysis relies on the connections between a group of variables that are independent and a single variable that is dependent. The following is the multiple regression equation for the variables considered in this study: Y=B0 +B1 X1+ B2 X2+

…+BnXn + E. Y is the response variable; X1 X2…Xn are the predictor variables; B0 B1 B2 …Bn are the partial regression coefficients and, E refers to the remaining error, or residual.

6.2.3.1. Multiple regression of MBTAM

Table 6. 10 Multiple regression model summary

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.755[a]	.570	.549	.54543

a. Predictors: (Constant) PU, PEOU, SSN, Trust, PH, PI, PSP

The results in Table 5.10 indicate the following:

- The R - value represents the correlation between the dependent and independent variable. A value greater than 0.4 is taken for further analysis. In this case, the value is .755, which is good.
- R-square shows the total variation in the dependent variable that could be explained by the independent variables. A value greater than 0.5 shows that the model is effective enough to determine the relationship. In this case, the value is .570, which is good.

Table 6. 11 multiple regression of ANOVA

ANOVA[a]						
Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	113.282	14	8.092	27.199	.000[b]
	Residual	85.382	287	.297		
	Total	198.663	301			

a. Dependent Variable: Intention to Use

b. Predictors: (Constant), PU, PEOU, SSN, Trust, PH, PI, PSP

The results in Table 5.11 indicate the following:

- P-value/ Sig value: Generally, 95% confidence interval or 5% level of the significance level is chosen for the study. Thus the p-value should be less than 0.05. In the above table, it is .000. Therefore, the result is significant.
- F-ratio: It represents an improvement in the prediction of the variable by fitting the model after considering the inaccuracy present in the model. A value is greater than 1 for F-ratio, yield efficient model. In the above table, the value is 27.199, which is good.

6.2.3.2. Test the hypothesis of the MBTAM regression model

This section of the study provides an overview of the multiple regression models and the significant status of the relationship between the independent and dependent variables. The section further provides a brief discussion of relationships among variables.

Table 6. 12 Multiple regression results between PH, PI, PSP, PEOU, PU, SSN, Trust (independent variables) and intention to use (dependent variable)

Coefficients[a]						
		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	T	Sig.
1	(Constant)	.026	.166		.154	.877
	PU	.350	.066	.324	5.278	.000
	POEU	.195	.063	.162	3.054	.011
	SSN	-.054	.038	-.070	-1.418	.157
	Trust	.350	.066	.311	5.103	.000
	PH	.132	.060	.126	2.196	.029
	PI	.196	.064	.301	3.070	.002
	PSP	.211	.052	.229	4.030	.000

a. Dependent Variable: Intention to Use

As the aim of this study is to measure the acceptance of biometric authentication technology on mobile devices, the analysis will first focus on the main variables of acceptance in our acceptance model followed by the remaining variables. The key variables of the customer's intention to use mobile biometric devices (Intention to use) are PEOU (β=0.162; $p<0.05$), PU (β=0.324; $p<0.05$), PH (β=0.126, $p<0.05$), PI (β=0.301; $p<0.05$), PSP (β=0.229; $p<0.05$), SSN (β=.-070; $p>0.05$) and Trust (β=0.311; $p<0.05$). The results in Table 6.12 indicate that Trust, PI and PU are the most important variables in explaining customer's intention to use mobile biometric devices (Intention to use). Intention to use on its own is a key variable to AUMBD with (β=0.177; $p<0.05$). It is indicated in the results that PEOU is the most important variable that explains PU (β=0.576; $p<0.01$) followed by SSN (β=0.180; $p<0.01$). It is indicated by the findings of this study that the relationship amongst Intention to use and other variables is statistically significant at the 5% level as their p-values are less than 0.05 ($p<0.05$) except for SSN. It is indicated by the results that the relationship between Intention to use and SSN is not statistically significant because the p-value is greater than 0.05.

Table 6. 13 Multiple regression results between reliability, privacy, security (independent variables) and trust (dependent variable)

Coefficients[a]						
		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	T	Sig.
1	(Constant)	1.207	.182		6.634	.000
	Reliability	.466	.052	.468	8.971	.000
	Privacy	.097	.086	.074	1.132	.258
	Security	.026	.083	.020	.316	.752

a. Dependent Variable: Trust

Reliability is the most important variable that explains trust with (β=0.468; $p<0.05$). It is indicated by the results that privacy (β=0.074; $p>0.05$) and security (β=0.020; $p>0.05$) are not important determinants of trust. The results of the regression analysis indicate that the relationship between trust and reliability is statistically significant at the 5% level with p=0.000

and less than 0.05 ($p<0.05$). It is further indicated by the results that the relationship between trust, privacy and security is not statistically significant because the p-values are greater than 0.05 ($p>0.05$).

Table 6. 14 Multiple regression results between identity theft, combining data (independent variables) and privacy (dependent variable)

Coefficients[a]						
		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	T	Sig.
1	(Constant)	1.276	.139		9.184	.000
	Identity theft	.277	.044	.340	6.330	.000
	Combining data	.109	.041	.144	2.679	.008

a. Dependent Variable: Privacy

It was found that identity theft with ($\beta=0.340$; $p<0.05$) and combining data with ($\beta=0.114$; $p<0.05$) is the determining factor of privacy. İdentity theft is the most important contributing factor to privacy out of all data protection elements, even though privacy on its own is not supported. İn all of the data protection elements, identity theft contributes the highest. The results of the regression analysis indicate that the relationship amongst privacy, identity theft and combining data is statistically significant at the 5% level and less than 0.05 ($p<0.05$).

Table 6. 15 Multiple regression results between intention to use (independent variables) and actual use (dependent variable)

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.114	.141		14.988	.000
	Intention to Use	.224	.072	.177	3.107	.002

a. Dependent Variable: Actual Use

The results of the regression analysis indicate that the relationship between actual use and intention to use is statistically significant at the 5% level and less than 0.05 ($p<0.05$). Thus, intention to use is an important factor of actual use of the mobile biometric device.

Table 6. 16 Multiple regression results between accuracy (independent variables) and PEOU (dependent variable)

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.679	.110		15.335	.000
	Accuracy	.085	.048	.102	1.779	.076

a. Dependent Variable: PEOU

The results of the regression analysis indicate that the relationship PEOU and accuracy is not statistically significant and the p-value is greater than 0.05 ($p>0.05$). Thus, Accuracy is not important determinant of PEOU.

Table 6. 17 Multiple regression results between PEOU, SSN, identity assurance (independent variables) and PU (dependent variable)

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.427	.132		3.228	.001
	POEU	.589	.048	.576	12.340	.000
	SSN	.128	.032	.180	3.961	.000
	Identity assurance	.010	.043	.011	.242	.809

a. Dependent Variable: PU

According to the proposed model for this study, PU is determined by three variables which are; PEOU (β=0.576; $p<0.05$), SSN (β=0.180; $p<0.05$) and identity assurance (β=0.011; $p>0.05$). Of all the determinants factor of PU, it was indicated by the results that PEOU contribute the highest followed by SSN. However, SSN on its own is not supported. It was further indicated by the results that identity assurance is not an important determinant of PU. The results of the regression analysis indicate that the relationship amongst PU and other variables is statistically significant at the 5% level as their p-values are less than 0.05 ($p<0.05$) except for identity assurance. It is indicated by the results that the relationship between PU and identity assurance is not statistically significant because the p-value is greater than 0.05.

Table 6. 18 Multiple regression results between functional elements (independent variables) and intention to use (dependent variable)

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.728	.149		4.868	.000
	Functional_elements	.167	.023	.390	7.329	.000

a. Dependent Variable: Intention_to_Use

The sum of functional elements of our model indicates that PEOU, PU and SSN altogether, strongly explain Intention to use with (β=0.390; $p<0.05$). Although SSN is not supported, the variable on its own influence PU, moreover the sum of all functional elements indicates a very strong influence on intention to use. Therefore, the conclusion cannot yet be made on whether the variable must be removed or not. The results of the regression analysis indicate that the relationship between intention to use and functional elements is statistically significant at the 5% level and the p-value is less than 0.05 ($p<0.05$).

Table 6. 19 Multiple regression results between social elements (independent variables) and intention to use (dependent variable)

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.392	.148		2.653	.008
	Social_elements	.220	.023	.490	9.734	.000

a. Dependent Variable: Intention_to_Use

The sum of the social elements of our model indicates that PH, PI and PSP altogether, strongly explain Intention to use with (β=0.490; $p<0.05$). All functional elements indicate a very strong influence on intention to use. The results of the regression analysis indicate that the relationship

between intention to use and social elements is statistically significant at the 5% level and the p-value is less than 0.05 ($p<0.05$).

Table 6. 20 Multiple regression results between social elements (independent variables) and intention to use (dependent variable*)*

Coefficients[a]						
		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig.
1	(Constant)	1.283	.208		6.163	.000
	DP	.181	.031	.323	5.914	.000

a. Dependent Variable: Trust

The sum of the data protection elements of our model indicates that identity theft, privacy and combining data altogether, strongly explain trust with ($\beta=0.323$; $p<0.05$). Although privacy is not supported, the variable on its own is influenced by identity theft and combining data, moreover the sum of all data protection elements indicates a very strong influence on trust. Therefore, the conclusion cannot yet be made on whether the variable must be removed or not. The results of the regression analysis indicate that the relationship between trust and data protection elements (DP) is statistically significant at the 5% level and the p-value is less than 0.05 ($p<0.05$).

Table 6. 21 Regression Model Summary values for all tested hypotheses

Dependent Variables	R	Acceptable
PU	.363	No
Trust	.497	Yes
Privacy	.368	No
AUMBD	.177	No
PEOU	.102	No
Dependent Variables	R^2	Effective
PU	.501	Yes
Trust	.247	No
Privacy	.135	No

AUBDM	.031	No
PEOU	.010	No

Table 6. 22 Summary of the ANOVA[a] values for all tested hypotheses

Dependent Variables	Sig.	Results is Significant
PU	.000	Yes
Trust	.000	Yes
Privacy	.000	Yes
AUBDM	.002	Yes
PEOU	.076	No
Dependent Variables	F	Efficient
PU	67.432	Yes
Trust	32.627	Yes
Privacy	23.374	Yes
AUBDM	9,652	Yes
PEOU	3.164	Yes

6.2.4.3. Final Mobile Biometric Technology Acceptance Model (MBTAM)

After the regression analysis was complete, the final Mobile Biometric Technology Acceptance Model (MBTAM) did not include identity assurance, accuracy and security since they were non-significant variables. The links that indicated the relationships amongst data protection elements (identity theft, privacy and combining data) were removed because privacy was not supported. However, the sum of the data protection elements was computed to find out how much they contribute towards trust altogether and it was found that there is a very strong relationship between data protection elements and trust. Thus, the elements will also form part of the proposed research model.

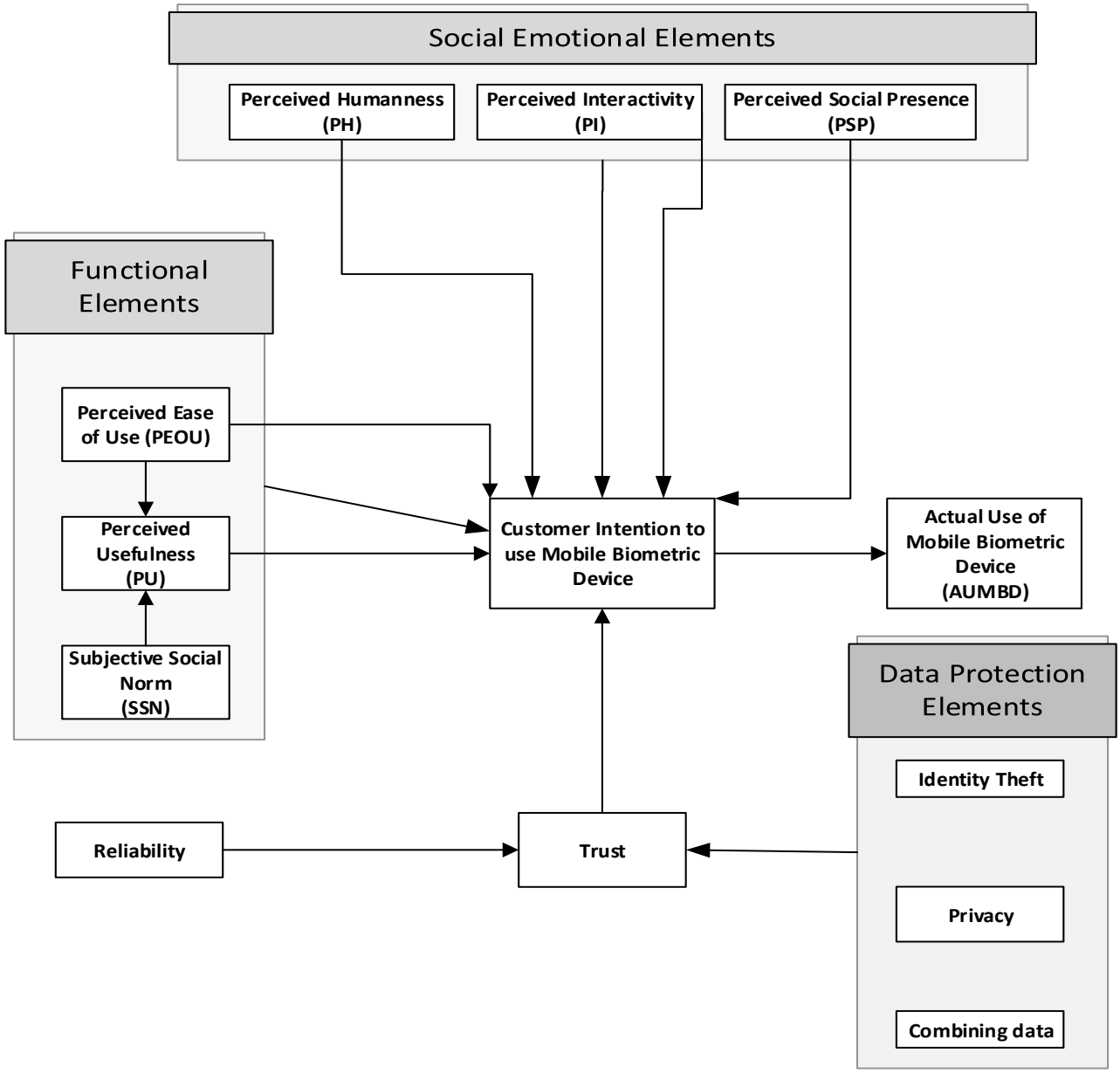


Figure 6. 3 MBTAM Model (Derived from Ho, Stephens and Jmieson, 2003 and Wirtz *et al.* 2020)

6.3. Conclusion

Data analysis processes have been presented in this chapter in two main phases. The first phase was focused on discovering the correlation relationship between model variables. The findings revealed that there is a significant relationship amongst the variables. The second phase presented multiple regression analysis results to discover any possible relationships amongst dependent and independent variables. The results indicated that some of the variables are not significant.

Chapter seven: Discussions of results

7.1. Introduction

This chapter will discuss the results obtained in chapter 6 into details. The main objective of this study is to find out the perception of the acceptance of biometric authentication security technology on mobile devices. This chapter will start by presenting the regression model of MBTAM and then later the hypotheses will be tested reviewing the determinants of acceptance of mobile biometrics. The presentation of the hypotheses will be in numerical order.

7.2. The presentation of the multiple regression results of MBTAM model

The figure below (Figure 7.1) presents the final MBTAM model after the non-significant variables and relationships were removed. The discussion will be based on all variables that are presented on the final MBTAM model and also those variables which were removed from the model and relationships since they might be important for further or future research.

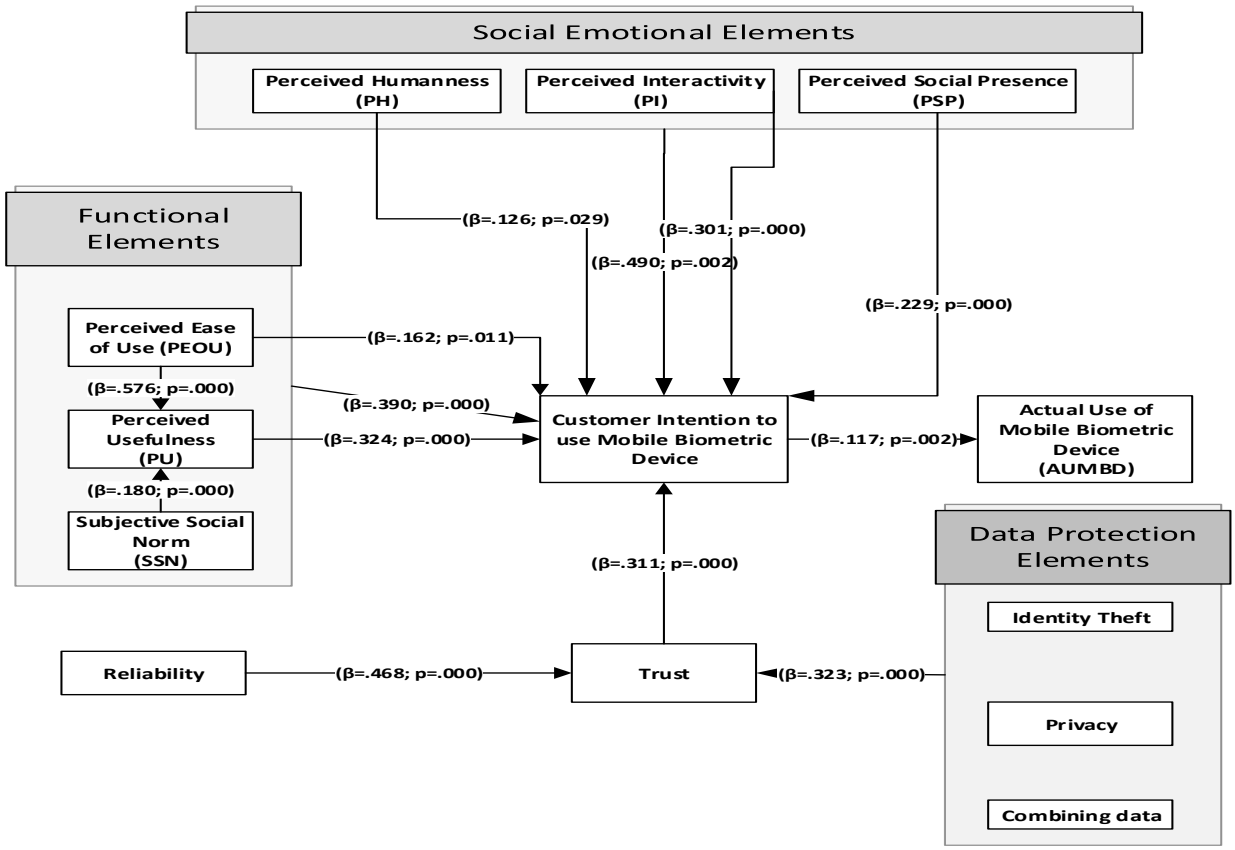


Figure 7. 1 MBTAM Mathematical Model (Derived from Ho, Stephens and Jmieson, 2003 and Wirtz *et al.* 2020)

7.3. Discussion per Hypothesis

7.3.1. Hypothesis 1

H_{01}: Perceived humanness has a positive influence on intention to use.

The significant value between perceived humanness and intention to use is positive at .029 which is less than .05. Therefore, this hypothesis is significant and can be supported as indicated by the obtained results.

The value of beta at .126 of these results also indicates the support for this hypothesis. The study conducted by Stock and Merkle (2018) on a comparison of innovation behaviour cues revealed that perceived humanness is an important determinant of intention to use. The results of the current study are supported by the results of Stock and Merkle (2018)'s study. It is indicated in the results that perceived humanness on its own contributes the lowest on customers' intention to use mobile biometric device, compared to all social emotional elements of the proposed model for the current study.

The results indicate that mobile users' perceived humanness determines their intention to accept and use mobile biometrics. It was revealed by the results of the current study that the customers will first need to be happy about the mobile biometric devices, be satisfied about mobile biometric devices and lastly understand these devices before they can accept and use these devices.

The analysis of data supports the results of the literature. Thus the hypothesis that perceived humanness has a positive influence on customers' intention to use mobile biometric devices is supported.

7.3.2. Hypothesis 2

H_{02}: Perceived interactivity has a positive influence on intention to use.

The significant value between perceived interactivity and intention to use is positive at .000 which is less than .05. Therefore, this hypothesis is significant and can be supported as indicated by the obtained results.

The value of beta at .301 of this hypothesis also indicates that the association between perceived interactivity and intention to use is good. Stock and Merkle (2018) conducted a study of a comparison of innovation behaviour cues. The results of their study revealed that perceived interactivity is an important determinant of intention to use. The results of the current study are supported by the results of Stock and Merkle (2018)'s study. It is indicated in the results that perceived interactivity on its own contributes the highest on customers' intention to use mobile biometric device, compared to all social emotional elements of the proposed model for the current study.

The results of the current study indicate that perceived interactivity plays a significant role in shaping the mobile users' willingness to accept and use mobile biometric devices. This means that perceived interactivity could have an influence on the degree to which mobile users perceive the existence of biometric authentication technology on mobile devices. Moreover, the results of the current study indicate that perceived interactivity affects the development of the consumer's intention to use mobile biometric devices. It is indicated by the obtained results of this study that perceived interactivity is an important and a very good determining factor of intention to use.

When carefully going through the obtained results from this study, it can be seen that users are willing to interact with biometric mobile devices. Mobile users are intending to accept biometric authentication technology on their devices if it will allow them to unlock their mobile devices easily without delays, if they will be allowed to have a full control over their devices and lastly if there will be a good communication between them and their mobile biometric devices.

The association between these two variables should be a focus area for biometric marketers. The results of the study reveal that perceived interactivity may be an effective benefit of mobile biometrics advertisement. Individuals will become increasingly interested in utilising mobile biometric devices.

The analysis of data supports the results of the literature. Thus the hypothesis that perceived interactivity has a positive influence on customers' intention to use mobile biometric devices is supported.

7.3.3. Hypothesis 3

H_{03}: Perceived social presence has a positive influence on intention to use.

The significant value between perceived social presence and intention to use is positive at .000 which is less than .05. Therefore, this hypothesis is significant and can be supported as indicated by the obtained results.

The value of beta at .229 of this hypothesis also indicates that the association between perceived interactivity and intention to use is good. The study conducted by Stock and Merkle (2018) on a comparison of innovation behaviour cues revealed that perceived social presence is an important determinant of intention to use. The results of the current study are supported by the results of Stock and Merkle (2018)'s study. It is indicated in the results that perceived social presence on its own contributes the second highest on customers' intention to use mobile biometric device, compared to all social emotional elements of the proposed model for the current study.

Social presence is defined as the degree to which a being believes that somebody is "actually present" (Heerink, Marcel, Krose, Evers and Wielinga, 2010). It is indicated by the results of the current study that mobile users can feel that they are with other social beings. Mobile users' perceived social presence determines their intention to accept and use biometric authentication technology in their devices.

The results of the current study revealed that mobile users perceive the presence of biometric mobile devices in the communication. It was found that mobile users will intent to use mobile

biometric devices if there is a sense of sociability with those devices, if there is a sense of human warmth and if there is a sense of human contact with mobile biometric devices.

The analysis of data supports the results of the literature. Thus the hypothesis that perceived social presence has a positive influence on customers' intention to use mobile biometric devices is supported.

7.3.4. Hypothesis 4

H_{04}: Perceived ease of use has a positive influence on intention to use.

The significant value between perceived ease of use and intention to use is positive at .011 which is less than .05. Therefore, this hypothesis is significant and can be supported as indicated by the obtained results.

The value of beta at .162 of this hypothesis also indicates that there is a significant association between perceived ease of use and intention to use. Ho, Stephens and Jamieson (2003)'s study revealed that perceived ease of use positively influence customers' intention to use biometrics. The study conducted by Sanchez-Franco (2010) also discovered that perceived ease of use has a positive influence on intention to use. Furthermore, Mohamed, Shaari, Ismail and Anuar (2018) conducted a study on mobile phone usage and these studies found that perceived ease of use has a positive influence on intention to use. The results of all the above-mentioned studies support the results of the current study. Perceived ease of use on its own contributes the second highest on intention to use compared to all functional elements of the study.

The results of this study indicate that the customers' intention to use biometric authentication technology on mobile devices is affected or determined by perceived ease of use. This means that the easier the authentication technology, the more the customers will intent to use it on mobile devices.

Previous studies indicated that people find it difficult to adopt new technology since it is not easy to use. This is a calling for IT decision-makers and developers on the development phase of the biometric security to ensure that the security is easy to use without complications. Thus, mobile users will intent to accept and use this technology on mobile devices.

The results of the data analysis support the findings of the literature. The hypothesis which predicted that perceived ease of use has a positive influence on customers' intention to use mobile biometric devices is supported.

7.3.5. Hypothesis 5

H_{05}: Perceived usefulness has a positive influence on intention to use.

The significant value between perceived usefulness and intention to use is positive at .000 which is less than .05. Therefore, this hypothesis is significant and can be supported as indicated by the obtained results.

The value of beta is high at .324 which indicates that there is a strong significant association between perceived ease of use and perceived usefulness. Perceived usefulness is known as the functional element of the TAM model as defined by Davis, Bagozzi and Warshaw (1989). Ho, Stephens and Jamieson (2003) found that perceived usefulness positively influence the customer's intention to accept and use biometric technology. These findings support the results of the current study. Liao *et al.* (2018) also discovered the same results that perceived usefulness directly influences customers' intention to accept and utilise a specific technology, which also supports the results of the current study. Compared to all functional elements of the proposed model, perceived usefulness contributes the highest towards customers' intention to accept and use the mobile biometric device.

This means that, as long as mobile device users believe that using biometric authentication technology on mobile devices will achieve the mobile devices' security access requirements then there is a high chance or higher possibility that customers' intention to accept and use biometric authentication technology on mobile devices will increase.

This relationship between perceived usefulness and intention to use should be carefully considered by developers during the development phase of the biometric authentication technology. This implies that developers should ensure that the developed biometric authentication technology achieves or meets the mobile devices' security access requirements in order to increase the possibility of the customers' intention to accept and use this technology when is applied on mobile devices.

The results of the data analysis support the findings of the literature. Thus, the hypothesis which states that perceived usefulness has a positive influence on customers' intention to use mobile biometric devices is supported.

7.3.6. Hypothesis 6

H_{06}: Subjective social norm has a positive influence on intention to use.

The significant value between subjective social norm and intention to use is positive at .157 which is greater than .05. Therefore, this hypothesis could not be supported as indicated by the obtained results of the data for this study. The beta value is also negative at -.070 which also indicates that the relationship is negative.

The previous study by Venkatesh, Morris, Davis and Davis (2003) found that subjective social norm (as social influence) directly influence customers' intention to use an innovation. Ho, Stephens and Jamieson (2003) also confirmed that subjective social norm (as subjective norm) has a positive influence on customers' intention to accept and use biometric technology. However, the study conducted lately by an, Ramayah and Amin (2015); Shan and King (2015) found that subjective social norm does not have an influence on the customer's intention to use any technology. They have reasoned that even if it may be right in principle or for individual innovation use, the conceptualization may not be reliable or trustworthy in a work space. Therefore, the outcomes of this study are in line with the outcomes of an, Ramayah and Amin (2015); Shan and King (2015).

Maruping, Bala, Venkatesh and Brown (2016) said that subjective social norm is when a being is influenced by "word of mouth" from a workmate or peer. According to the findings of this study, mobile users' willingness to accept and use biometrics on mobile devices is not determined by a word of mouth from peers or fellow workers. This indicates that the subjective social norm that is experienced by the mobile users negatively contribute towards users' intention to accept biometric authentication on mobile devices. Compared to all functional elements of the proposed model for this study, subjective social norm proved to be a weaker determinant of customers' intention to use mobile biometric device.

This is a revelation to biometric marketers who may be guided by these results to focus on subjective social norm and intention to use. They should be aware that their perceived social pressure or motivation might not succeed in making mobile users to comply with their views of biometric authentication on mobile devices. This means that their perceived social pressure might not influence customers' intention to accept biometric authentication technology on mobile devices.

The results of the data analysis support the findings of the literature. However, the hypothesis which predicted that subjective social norm has a positive influence on customers' intention to use mobile biometric devices is not supported.

7.3.7. Hypothesis 7

H_{07}: Trust has a positive influence on intention to use.

The significant value between trust and intention to use is positive at .000 which is less than .05. Therefore, this hypothesis is significant and can be supported as indicated by the obtained results.

The value of beta at .311 of this hypothesis also indicates that there is a significant association between trust and intention to use. Giesing (2020) described concerns that affect consumer expectations of biometrics usage, but his research was constrained by the context of Electronic Business. Giesing (2020) described social factors such as privacy, trust, and fraud as affecting biometric adoption. The results of the study found that trust was an important determinant of customer's intention to adopt biometrics. The findings of the current study are supported by Giesing (2020)'s study.

Numerous researchers conducted studies on the adoption and acceptance of biometrics and found that customers or users are rapidly growing an appetite for the use of biometric authentication technologies. In this study it was found that, mobile users are also willing to accept biometric authentication technology, but their willingness to accept this technology is determined by the trust. It was indicated by the findings that as long as biometric authentication technology will be a trusted security on mobile devices in terms of data security, privacy and reliability, then chances are high that mobile users will accept biometric authentication technology on their

mobile devices.

The fact that mobile device users are ready to accept biometric authentication technology on mobile devices is indeed great news. However, the biometric developers need to ensure that the arrival of proven biometric authentication technology guarantees to resolve one of the major challenges which incorporate trust. Whether mobile users will accept biometric authentication technology on their devices is determined by trust. The developers need to ensure that biometrics can withstand fraudulent activity and build a strong level of trust among consumers; this will increase the possibility of the acceptance of biometric authentication technology on mobile devices. Burt (2020) indicated that trust in biometrics is the theme for top news stories. The market is apparently deep into technology and coming up with different solutions for improving the biometric security so that it can gain even more of users' trust (Capps, 2019). Trust is the most important determinant of customers' intention to accept an innovation.

The results of the data analysis support the findings of the literature. Thus, the hypothesis that trust has a positive influence on customers' intention to accept and use biometric authentication technology on mobile devices is supported.

7.3.8. Hypothesis 8

H_{08}: Perceived ease of use has a positive influence on perceived usefulness.

The significant value between perceived ease of use and perceived usefulness is positive at .000 which is less than .05. Therefore, this hypothesis is significant and can be supported as indicated by the obtained results.

The value of beta is high at .576 which indicates that there is a significant association between perceived ease of use and perceived usefulness. In the context of biometrics Ho, Stephens and Jamieson (2003) defined perceived ease of use as "the degree to which a being believes that utilising a specific framework would be free of effort". This definition remains the way Davis, Bagozzi and Warshaw (1989) defined perceived ease of use. The definition was not modified since it still suits the context of biometrics.

Ho, Stephens and Jamieson (2003) confirmed that perceived usefulness is determined by

perceived ease of use and this supports the findings of this study. Lee, Park, Kang and Park (2009) also confirm that perceived ease of use is the determining factor of perceived usefulness. This means that mobile device users might be directly impacted if biometric authentication technology will be easy to use when implemented on mobile devices.

On the biometric development side, this positive association between perceived ease of use and perceived usefulness should be an area of focus. This means that if the biometric developers make the biometric authentication technology easier to use, then mobile users might accept biometric mobile devices with the belief that it will enhance their job performance since perceived ease of use influence the customer's perceived usefulness of mobile biometrics.

The results of the data analysis are in line with the literature. Thus, the hypothesis which states that perceived ease of use has a positive influence on the perceived usefulness of mobile biometric acceptance is supported.

7.3.9. Hypothesis 9

H_{09}: Subjective social norm has a positive influence on perceived usefulness.

The significant value between subjective social norm and perceived usefulness is positive at .000 which is less than .05. Therefore, this hypothesis is significant and can be supported as indicated by the obtained results.

The value of beta at .180 of this hypothesis also indicates that there is a significant association between subjective social norm and perceived usefulness. Thus, users of mobile devices believe that peers and peoples' influence are important to how they think and decide. According to the findings of this study, it is shown that users believe that peers and people's influence determine their perceived usefulness of mobile biometric devices. The results of this study further indicate that the subjective social norm that is experienced by the mobile users support the acceptance of biometric authentication technology on mobile devices, thus mobile users will be more likely to accept this technology. Moreover, mobile users are more likely to respond to subjective social norm when there is a security enhancement on those devices.

Perceived usefulness is one of the functional elements of TAM, and biometric technology

acceptance model uses social influence as subjective social norm. Ho, Stephens and Jamieson (2003) discovered that subjective social norm positively influence perceived usefulness. This indicates that the results are supported by the findings of Ho, Stephens and Jamieson (2003).

This association between subjective social norm and perceived usefulness should be a potential area of focus for biometric marketers. Biometric marketers may be able to influence users of mobile devices and other technologies to accept biometric authentication technology since perceived usefulness can be determined by subjective social norm.

Therefore, the analysis of data supports the results of the literature which in turn indicate that the hypothesis that subjective social norm has a positive influence on the perceived usefulness of mobile biometric acceptance is supported.

7.3.10. Hypothesis 10

H_{10}: Accuracy has a positive influence on perceived ease of use.

The significant value between accuracy and perceived ease of use is positive at .076 which is greater than .05. Therefore, this hypothesis could not be supported as indicated by the obtained results of the data for this study. The beta value is positive at .102 which also indicates that it is not significant.

Too much research has been conducted on the technical issues of biometric authentication technology, such as performance and accuracy of the system (Gutkowski, 2004). Accuracy, on the study conducted by Ho, Stephens and Jamieson (2003) was defined as the degree to which the system is capable of matching a biometric sample with its pre-existing template accurately in a real world setting. They further mentioned that the accuracy of a biometric framework is dependent on its rate of errors. The findings of their study revealed that accuracy is the most important determinant of perceived ease of use.

However, the results of this study show that accuracy is not an important determinant of perceived ease of use. This means that the issues associated with the accuracy of the biometric authentication technology do not affect the mobile users' perceived ease of use of this technology on mobile devices. The fact that there might not be data consistency on this security

database and the functions of this biometric authentication technology on mobile devices might not be well integrated, does not mean that users will not find this technology easy to use on mobile devices. However, the researcher suggests that further research must be conducted to measure the accuracy of the biometric authentication technology on mobile devices.

The results of the data analysis contradict with the findings of the literature. Thus, the hypothesis that accuracy has a positive influence on customers' perceived ease of use of mobile biometric devices is not supported.

7.3.11. Hypothesis 11

H_{11}: Identity assurance does not have an influence on perceived usefulness.

The significant value between identity assurance and perceived usefulness is positive at .809 which is greater than .05. Therefore, this hypothesis can be supported as indicated by the obtained results of the data for this study. The beta value is positive at .011 which also supports the hypothesis.

Ho, Stephens and Jamieson (2003) extended TAM2 to include identity assurance as one of the determining factors of perceived usefulness. The findings of their study revealed that identity assurance is an influential determinant of perceived usefulness, and it was found to be the main reason why biometrics are adopted. In the context of biometrics, identity assurance is defined as the assurance that only authorised individuals are given access (Ho, Stephens and Jamieson, 2003).

The results of this study found that identity assurance is not a determining factor of perceived usefulness. The relationship between the two variables is not significant. This indicates that the assurance that only authorised individuals will be granted access by the biometric authentication technology to mobile devices does not affect the customers' perceived usefulness. It is further indicated that even if each user of the mobile biometric device are sure or not sure about the system having unique user traits and whether the user traits will match biometric user field or not, still this will not affect the users' perceived usefulness.

The results of the data analysis contradict with the findings of the literature. However, the

hypothesis that identity assurance does not have influence on customers' perceived usefulness of mobile biometric devices is supported.

7.3.12. Hypothesis 12

H_{12}: Intention to use has a positive influence on actual use.

The significant value between intention to use and actual use is positive at .002 which is less than .05. Therefore, this hypothesis is significant and can be supported as indicated by the obtained results.

The value of beta is at .117 which indicates that there is a good significant association between perceived ease of use and perceived usefulness. Turner *et al.* (2010) conducted a study to determine the capability of the TAM model in predicting the actual use of a technology. The findings of the study revealed that intention to use is a determining factor of actual use. Moreover, the study conducted by Horton, Buck, Waterson and Clegg (2013) found that the greater the customers' intention to use a technology the greater the actual use. The findings of this study showed that intention to use can determine or predict the actual use of the system. Therefore, the result of this hypothesis is supported or in line with Turner *et al.* (2010) and Horton, Buck, Waterson and Clegg (2013)' studies.

According to Nursiah (2020), intention to use an innovation is a behavioural aptness to carry on with its utilisation. The findings of this study indicated that the users are willing to use mobile biometric devices continuously. From the findings of this study it can be concluded that mobile users desire to accept and use biometric authentication technology on their mobile devices.

The relationship between customers' intention to use mobile biometric device and the actual use of the mobile biometric device indicates that intention to use is a way of behavioural intention to trend utilising a new system that is applied in an organisation or an institution. The findings of this study revealed that the customers' intention to use mobile biometric devices determines or predict the actual use of the mobile biometric devices.

The results of the data analysis support the findings of the literature. Thus, the hypothesis which states that the customers' intention to use mobile biometric device has a positive influence on the

actual use of mobile biometric devices is supported.

7.3.13. Hypothesis 13

H_{13}: Reliability has a positive influence on trust.

The significant value between reliability and trust is positive at .000 which is less than .05. Therefore, this hypothesis is significant and can be supported as indicated by the obtained results.

The value of beta at .468 of this hypothesis also indicates that there is a significant association between reliability and trust. In the biometric context Ho, Stephens and Jamieson (2003) defined reliability as "the probability that the system remains successful (does not fail) in achieving its intended objectives".

Shanab and Talfha (2015) conducted a study on the adoption and internet banking. The study hypothesized that reliability (as perceived reliability) has a positive influence on trust. The tests were made and it was found that their hypothesis was supported. Therefore, the study conducted by Shanab and Talfha (2015) supports the findings of the current study. The current study found that reliability is an important determinant of trust. Compared to privacy and security as determining factors of trust, reliability contributes the highest.

The results of this study reveal that reliability strongly determines or influence the mobile users' trust on biometric authentication technology. This means that the trust of mobile users of biometric authentication technology depends on the quality of trustworthiness or consistence performance of the system. It is therefore indicated that the higher the reliability of the system the greater the trust it will gain.

The results of the data analysis support the findings of the literature. Thus, the hypothesis that reliability has a positive influence on customers' trust for biometric authentication technology on mobile devices is supported.

7.3.14. Hypothesis 14

H_{14}: Security has a direct influence on trust.

The significant value between security and trust is positive at .752 which is greater than .05. Therefore, this hypothesis could not be supported as indicated by the obtained results of the data for this study. The beta value is positive at .020 which indicates that security contributes only 2% on trust. The association is therefore proving to be too much weak.

According to Biometrics (2020) security is associated with the integrity, confidentiality and availability of the data that is being processed and stored by a system. In the context of biometrics, security is determined by factors such as the ease of counterfeit, the possibility of replay attacks and the susceptibility to brute-force attacks (Biometrics, 2020).

Ramos, Ferreira, Freitas and Rodrigues (2018) conducted a study to measure the effect of trust in the intention to use mobile banking. The study found that security (as perceived security) has a direct and positive influence on trust. However, the results of the current study indicate that security is not a determinant of trust. Compared to privacy and reliability, security contributes the lowest on trust.

Therefore, this indicates that security does not determine the trust of mobile users on the acceptance of biometric authentication technology. For this study the results indicate that the security of the mobile devices does not go hand in hand with the trust that they have towards biometric authentication technology. Numerous studies have confirmed that trust of the system depends on security. Thus, the researcher calls for further research to be conducted to find out the relationship between trust and security of the biometric authentication technology on mobile devices.

The results of the data analysis contradict with the findings of the literature. Thus, the hypothesis that security has a direct influence on customers' trust of mobile biometric devices is not supported.

7.3.15. Hypothesis 15

H_{15}: Privacy has a positive influence on trust.

The significant value between privacy and trust is positive at .258 which is greater than .05. Therefore, this hypothesis could not be supported as indicated by the obtained results of the data for this study. The beta value is positive at .074 which indicates that privacy contributes the second highest compared to security and reliability on trust. However, the association proves to be weaker.

Individual privacy turns out to be one of the main concerns persons have when considering biometric authentication security technology than traditional authentication techniques (Ho, Stephens and Jamison, 2003). Thus, privacy shapes people's trust to the mobile biometric device (Kyrezis, 2010). In the context of biometrics, Ho, Stephens and Jamieson (2003) defined privacy as the disruption and individual's ability to control personal information. The study conducted by Ramos, Ferreira, Freitas and Rodrigues (2018) on measuring the effect of trust in the intention to use mobile banking, found that privacy (as perceived privacy) has a direct and positive effect on trust. However the results of the current study revealed that privacy is not a determinant of trust.

The results of this study indicate that privacy does not determine mobile users' trust on biometric authentication technology. This further indicates that in the current study, privacy is not a concern for mobile users. However, the researcher proposes that further research must be conducted to determine the relationship between privacy and trust of mobile users of biometric authentication security technology.

The results of the data analysis contradict with the findings of the literature. Thus, the hypothesis that privacy has a positive influence on customers' trust of mobile biometric devices is not supported.

7.3.16. Hypothesis 16

H_{16}: Identity theft has a positive influence on privacy.

The significant value between identity theft and privacy is positive at .000 which is less than .05 and supported. The beta value is positive at .340 which indicates that there is a positive association between these two variables. Therefore, the support for this hypothesis can be supported as indicated by the obtained results.

The study conducted by Ho, Stephens and Jamieson (2003) highlighted some issue associated with privacy and identity theft was one of those issues. The results of their study revealed that identity theft is an important determinant of privacy. The result of this hypothesis is supported by Ho, Stephens and Jamieson (2003)'s study. Compared to combining data, privacy contributes the highest towards privacy.

The findings of this study show that mobile users support the fact that when identity theft is not a priority issue, this will result in an exposure of unwanted information. Mobile users seem to be well educated and more informed about the necessity to protect individual data and it is a good thing. Furthermore, the results indicate that mobile users' wariness that unauthorised use of their personal data from their mobile biometric device can damage their reputation and their fear of that somebody can unlock their mobile devices easily has a direct impact on their data privacy.

Therefore, this serves as a calling to the biometric developers that the biometric security for mobile phones must be tight and strict to avoid data breaches. This will make users not to worry about their personal data security or privacy which will in return contribute to good trust of this technology by the users. Biometric authentication technology needs to ensure a strong data protection.

The results of the data analysis support the findings of the literature. Thus, the hypothesis that identity theft has a positive influence on privacy' is supported.

7.3.17. Hypothesis 17

H_{17}: Combining data has a positive influence on privacy.

The significant value between combining data and privacy is positive at .008 which is less than .05. Therefore, this hypothesis is significant and can be supported as indicated by the obtained results.

The value of beta at .144 of this hypothesis also indicates that there is a significant association between combining data and privacy. The study conducted by Ho, Stephens and Jamieson (2003) found that combining data is one of the determining factors of privacy. In their study, combining data was found to be one of the issues associated with data privacy. Therefore, they have indicated that combining data concern the possibility that data from disparate databases might be combined into larger databases. The results of the current study are in line with Ho, Stephens and Jamieson (2003)'s study.

The association between these two variables reveals that combining data is an important determinant of privacy. It is very much important to consider how biometric system store and merge individual data security with individual mobile data (the merging of the two databases). Too much mix of data from large databases might result in identity theft, but all this will be the results of how the two databases (mobile database and biometric database) combine their data. Compared to identity theft, combining data contributes the lowest towards privacy. The results indicate that mobile users have concerns about biometric security's responsibility of combing their login details on their mobile devices.

The results of the data analysis support the findings of the literature. Thus, the hypothesis that combining data has a positive influence on privacy is supported.

7.3.18. Hypothesis 18

H_{18}: Functional elements have a positive influence on intention to use.

The significant value between functional elements and intention to use is positive at .000 which is less than .05. Therefore, this hypothesis is significant and can be supported as indicated by the obtained results.

The value of beta at .390 of this hypothesis also indicates that there is a significant association between functional elements and intention to use. Functional elements in the proposed model for the current study include PEO, PU and SSN. The researcher saw it necessary to add or to sum together all functional elements to determine their total strength toward customers' intention to use mobile biometric devices. It was found that functional elements contribute a lot and are considered as important determinants of customers' intention to use mobile biometric devices. This is the more reason why the conclusion was drawn by the researcher to keep SSN even if on its own is not supported. Adding functional elements together may also be useful in future research. Compared to social emotional elements, functional elements contribute the second highest towards customers' intention to use mobile biometric devices.

Thus, the hypothesis which states that functional elements have a positive influence on customers' intention to use mobile biometric devices is supported.

7.3.19. Hypothesis 19

H_{19}: Social emotional elements have a positive influence on intention to use.

The significant value between social emotional elements and intention to use is positive at .000 which is less than .05. Therefore, this hypothesis is significant and can be supported as indicated by the obtained results.

The value of beta at .490 of this hypothesis also indicates that there is a significant association between social emotional elements and intention to use. Social emotional elements in the proposed model for the current study include PH, PI and PSP. The researcher saw it necessary to add or to sum together all social emotional elements to determine their total strength toward customers' intention to use mobile biometric devices. It was found that social emotional

elements contribute a lot and are considered as important determinants of customers' intention to use mobile biometric devices. Summing social emotional elements together may also be useful in future research. Compared to functional elements, social emotional elements contribute the highest towards customers' intention to use mobile biometric devices.

Thus, the hypothesis which states that social emotional elements have a positive influence on customers' intention to use mobile biometric devices is supported.

7.3.20. Hypothesis 20

H_{20}: Data protection elements have a positive influence on trust.

The significant value between data protection elements and trust is positive at .000 which is less than .05. Therefore, this hypothesis is significant and can be supported as indicated by the obtained results.

The value of beta at .323 of this hypothesis also indicates that there is a significant association between data protection elements and trust. Data protection elements in the proposed model for the current study include combining data, privacy and identity theft. The researcher saw it necessary to add or to sum together all data protection elements to determine their total strength to trust. It was found that data protection elements contribute a lot and are considered as important determinants of trust. Summing data protection elements together may also be useful in future research. Compared to reliability, data protection elements contribute the second highest towards trust.

Thus, the hypothesis which states that data protection elements have a positive influence on trust is supported.

7.4. Summary

Table 7.1 provides a summary of the results for this chapter.

Hypotheses	P-value	Supported
H_{01}: Perceived Humanness (PH) has a positive influence on intention to use.	P = 0.029 P < 0.05	Yes
H_{02}: Perceived Interactivity (PI) has appositive influence on intention to use.	P = 0.000 P < 0.05	Yes
H_{03}: Perceived Social Presence (PSP) has a positive influence on intention to use.	P = 0.000 P < 0.05	Yes
H_{04}: Perceived Ease of Use (PEOU) has a positive influence on intention to use.	P = 0.011 P < 0.05	Yes
H_{05}: Perceived Usefulness (PU) has a positive influence on intention to use.	P = 0.000 P < 0.05	Yes
H_{06}: Subjective Social Norm (SSN) has a positive influence on intention to use.	P = 0.157 P > 0.05	No
H_{07}: Trust has a positive influence on intention to use.	P = 0.000 P < 0.05	Yes
H_{08}: Perceived Ease of Use (PEOU) has a positive influence on Perceived Usefulness (PU).	P = 0.000 P < 0.05	Yes
H_{09}: Subjective Social Norm (SSN) has a negative influence on Perceived Usefulness (PU).	P = 0.000 P < 0.05	Yes
H_{10}: Accuracy has a positive influence on Perceived Ease of Use (PEOU).	P = 0.076 P > 0.05	No
H_{11}: Identity assurance has a positive influence on Perceived Usefulness (PU).	P = 0.809 P > 0.05	No
H_{12}: Intention to use has a positive influence on Actual Use of Mobile Biometric Devices (AUMBD).	P = 0.002 P < 0.05	Yes
H_{13}: Reliability has a positive influence on Trust.	P = 0.000 P < 0.05	Yes
H_{14}: Security has a positive influence on Trust.	P = 0.752	No

	P > 0.05	
H_{15}: Privacy has a positive influence on Trust.	P = 0.258 P > 0.05	No
H_{16}: Identity theft has a positive influence on Privacy.	P = 0.000 P < 0.05	Yes
H_{17}: Combining data has a positive influence on Privacy	P = 0.008 P < 0.05	Yes
H_{18}: Functional elements have a positive influence on intention to use	P = 0.000 P < 0.05	Yes
H_{19}: Social elements have a positive influence on intention to use	P = 0.002 P < 0.05	Yes
H_{20}: Data protection elements have a positive influence on trust	P = 0.000 P < 0.05	Yes

Table 7.1: Summary of the results

7.5. Conclusion

This chapter discussed all the hypotheses of the proposed study into details. The relationships between variables were proven to be supported, however, not all of them. The researcher took a decision to remove all those variables that were not supported and suggested future research to be conducted on them.

Chapter eight: Conclusions and recommendations

8.1. Introduction

In this chapter the summary, findings and applications of the current study are presented based on the data that was analysed from the previous chapter. Some limitations of the current study have been identified. The study was carried out with the main aim of finding out the perception of acceptance of biometric authentication security technology on mobile devices. The current study sought to provide answers to the following research questions:

- What has been done, according to the literature, to measure user acceptance of technology?
- What model can be proposed to measure the acceptance of biometric authentication technology on mobile devices?
- How does one measure the effect of every variable of the model in the acceptance of biometric authentication technology on mobile devices?

8.2. Summary of the current study

8.2.1. Methodology

A deductive research approach was chosen for this quantitative study. The population of this study included citizens in South Africa from Johannesburg (Vanderbijlpark) only. The pilot study was conducted to test the questionnaire and reduce imperfections and to check whether the respondents understand the questions before they can be distributed. Only 10% of the sample size was used to conduct a pilot study. This study used a survey based questionnaire to collect data from the respondents because of its effectiveness at being practical and less costly. The Simple random sampling technique was used to select the study participants. The response rate was 98% of the expected population, which is a total of 302 valid responses. To analyse data, descriptive statistics were used and the significance level of p-value = 0.05 was used to test the reliability of the relationship between variables.

8.2.2. Objectives of the study

The main purpose of this study was to determine the perception of the acceptance of biometric authentication technology on mobile devices. The sub-objectives of this study were to:

- To study and determine what was done, according to the literature, to measure user acceptance of technology.
- To propose a model that could be used to measure the acceptance of biometric authentication technology on mobile devices.
- To measure the effect of every variable of the model in the acceptance of biometric authentication technology on mobile devices.

The findings for each objective will be discussed individually as follows:

Objective 1

- To study and determine what was done, according to the literature, to measure user acceptance of technology.

Technology acceptance has become a key issue in the research field. Acceptance on its own can be generally described as an opposition to the term denial and it refers to a positive choice to utilise a specific technology. Academicians and practitioners have developed an interest in recognizing the factors that affect users' acceptance or denial of technology. It was found in the literature that when users or clients are introduced to new technology, numerous factors that influence their decisions about how and when they will use it were noted.

According to the findings of the literature, theories and models were developed by numerous researchers to explain and examine the user acceptance of technology and every model or theory described user acknowledgement. It was through those theories and models that the user acceptance of technology was able to be measured. This provided information from the literature review in chapter two affirms that the above objective has been successfully achieved.

Objective 2

- To propose a model that can be used to measure the acceptance of biometric authentication technology on mobile devices.

The importance of theories and models that predict and characterize information technology adoption and use has grown in tandem with the growing popularity of customers' responses to IT. Researchers acknowledged and utilise theories and models to evaluate the acceptance of technology.

Numerous studies utilised different frameworks to conduct their investigations; nevertheless, in this study Technology Acceptance Model (TAM) was proposed as the suitable model that can be used to measure acceptance of biometric authentication technology on mobile devices. One of the most influential extensions is this model. Its founders emphasised that the secret to increasing usage was to first increase acceptance of information technology, which could be assessed by asking people about their potential plans to use information technology.

TAM theory has gone through several revisions and improvements. Researchers added or removed some variables to upgrade this model so that it can fit their studies. However, other researchers argue that TAM and its revised versions are not inappropriate for all applications since some main constructs like perceived risk are removed.

As TAM continued to be modified, researchers conducted the study on the acceptance of biometric authentication technology which they have extended or modified TAM. They named the model Biometric Technology Acceptance Model (BTAM). This model was derived from the original TAM model. For the purpose of the current study, the researcher adapted this model to measure the acceptance of biometric authentication technology on mobile devices. The name of this model was modified to Mobile Biometric Technology Acceptance Model (MBTAM) by the researcher.

The findings of this objective revealed that TAM is the suitable model to measure the acceptance of biometric authentication technology on mobile devices. Good results were obtained from the respondents through the use of this model with a high percentage of respondents. Thus, MBTAM

that was proposed in chapter four is the proposed model that can be used to determine the acceptance of biometric authentication on mobile devices.

Objective 3

- To measure the effect of every variable of the model in the acceptance of biometric authentication technology on mobile devices.

Using data that were collected from respondents made it possible to measure the effect of all variables of the proposed model. According to the respondents' information, other variables proved to be suitable and capable of measuring the acceptance of biometric authentication technology on mobile devices. However, it was found that only three variables were not significant. These lead to the removal of those variables from the final MBTAM model.

The variables that were supported include PH, PI, PSP, PEOU, PU, SSN, trust, intention to use, reliability, identity theft, combining data, and privacy. In measuring all variables, the findings revealed that accuracy, identity assurance and security were not supported. These resulted in the removal of those variables from the final MBTAM model. However, the researcher recommends further research to be conducted to measure those variables.

According to the findings of this study the purpose of measuring the effect of all variables of the proposed model was fulfilled. The findings revealed that of all social emotional elements of the proposed model, perceived interactivity (PI) contributed the highest towards the user's intention to accept and use mobile biometric devices. This variable was followed by PSP and PH respectively. In measuring the functional elements of the model it was found that PU contributes the highest, followed by PEOU and SSN respectively. The data protection elements were summed together in order to measure the level of their influence towards trust and they revealed a very strong relationship. According to the findings of this study, reliability is a good determinant of trust and trust is an important determining factor of the customer's intention to use mobile biometric devices.

In measuring the effect of all variables of the proposed MBTAM model, the researcher saw it necessary to compute and find out the total strength of the social emotional elements (sum of PH, PI and PSP), functional elements (sum of PEOU, PU and SSN) and data protection elements

(sum of identity theft, combining data and privacy). It was found that all those variables combined together, they contribute very well towards customers' intention to use mobile biometric devices. Social emotional elements contributed the highest, followed by functional elements and data protection elements, respectively. The above provided information affirms that the purpose was successfully fulfilled through chapter six.

8.2.3. Questions of the study

The findings for each research question will be discussed individually as follows:

Question 1

- What has been done, according to the literature to measure user acceptance of technology?

In this current study, it was revealed by the findings of the literature review that theories and models were developed by various researchers in order to explain and evaluate the user acceptance of technology. These theories and models were developed to measure the user acceptance of technology. With this above information from the literature, an answer for this research question was provided. Thus, the first research question was successfully answered.

Question 2

- What model can be proposed to measure the acceptance of biometric authentication technology on mobile devices?

The literature and related studies suggested that the technology acceptance model (TAM), is the suitable model that can be proposed to measure technology acceptance. Thus, TAM was proposed for this current study to measure acceptance of biometric authentication technology on mobile devices. This indicates that the second research question for this study was successfully answered.

Question 3

- How does one measure the effect of every variable of the model in the acceptance of biometric authentication technology on mobile devices?

In order to successfully measure the effect of each variable of the proposed model for the current study, a survey questionnaire was distributed to participants of the study in order to gather information that can help in measuring the effect of each variable of the model. The data that was collected from participants were put into SPSS in order to perform the calculations and determine the correlation and regression analysis. By determining the relationships between variables of the model for the current study, the researcher was able to measure the effect of each variable in the model. Thus, this research question was successfully answered.

8.2.4. Answering the main purpose and research questions of the study

The main objective of the study

- To determine the perception of the acceptance of biometric authentication technology on mobile devices.

The survey questionnaire was distributed to the study participants in order to find out their awareness, experience, understanding, willingness, and opinions about biometric authentication technology and its implementation on mobile devices. This is what was done by the researcher in order to determine the perception of acceptance of biometric authentication technology on mobile devices. Thus, this objective was successfully achieved.

The main research question of the study

- What is the perception of the acceptance of biometric authentication technology on mobile devices?

The results of the current study indicated that the majority of respondents are aware of the biometric authentication technology. However, it was only few participants that were not aware of the existence of this authentication technology. According to the participants of this study, biometric authentication technology, would be suitable for mobile devices. It was indicated by the findings of this study that the majority of the respondents prefer to use mobile biometric

devices. However, only a few indicated that they are not sure if they would use these devices due to security reasons.

According to the results of this study, the majority of the respondents understand biometric authentication technology and are willing to accept it on their mobile devices. Even if participants are aware of this authentication technology, they do not have too much experience on biometric mobile devices. It was revealed by the results of the current study that biometric authentication technology has a high chance of acceptance on mobile devices by users. Thus, the main research question of this study was successfully answered.

8.3. Findings

8.3.1. Context findings

It was revealed by the findings of this study from the literature review that there are only a few studies that measure the acceptance of biometric authentication technology on mobile devices. The findings of this study affirm that the study on the acceptance of technology on mobile devices is recent. The characteristics of the population used in this study are similar to other related studies in the literature review. The evaluation instruments that were used to gather data for this study and the research design together with procedures are also the same as other related studies in the literature review.

The findings of the current study agreed with the findings or existing literature, however, only a few findings contradict with the findings of the literature. Moreover, the findings of the current study extend the previous research and they solve and clarify the contradictions in the literature.

8.3.2. Implication findings

The implications of the findings in this study consider the following three areas:

8.3.2.1. Theory

The findings of this study are consistent with the current theories in the research field. However, this consistency applies to only a few of the current study findings. Other findings improve the findings of the related studies. Furthermore, the results of the current study, improve the proposed theoretical framework.

8.3.2.2. Research

In terms of research, the current study helped to improve or advance the research methodology. The study brought the understanding of new confounding variables, measurement issues and issues associated with the design. This study contributed by providing the mathematical framework that can be used to measure user acceptance of technology.

8.3.2.3. Practice

The findings of the current study suggest high level of acceptance of biometric authentication technology on mobile devices. A strong association was found between biometrics, mobile devices and users. Statistically significant relationships between the variables of the proposed model were found (p-value of 0.05)

In the professional field, these findings can be used by developers and biometric marketers to increase the acceptance and usage of biometric authentication technology on mobile devices. Researchers who wish to carry out their studies on the acceptance of biometric authentication technology on mobile devices can as well use the findings of the current study to improve their studies. The findings of this study could lead to positive changes in the way professionals do things.

8.4. Limitations of the current study

This study ha limitations that motivate the necessity for further research in this area. Some limitations that were identified are as follows.

- This study focused specifically on the acceptance of biometric authentication technology on mobile devices only.

- The second limitation of this study concerns the gender and the age of the respondents. The majority of the respondents were between 20 and 30 years and were male. This brought about an issue of unbalanced results. Generally, both male and female of different age groups nowadays are using mobile devices which need better security.

- The conceptual framework used in this study, was used only to measure the acceptance of biometric authentication technology only on mobile devices.

- The type of mobile devices used by participants had influence on the obtained results of this study.

8.5. Recommendations for further research

- Further research needs to be conducted on the acceptance of biometric authentication technology on other devices not only mobile devices.

- In future, the researchers in this field need to ensure the balancing of gender and age.

- In future, the researcher recommends the use of this conceptual framework to measure the acceptance of biometric authentication technology on other devices.

8.6. Summary of the chapter

This survey aimed to find out the perceptions as to the acceptance of biometric authentication technology on mobile devices. The model that was utilised in this survey attested to be valid, suitable and supported. The researcher recommended that further research must be conducted, particularly utilising supported variables in the model. The discoveries of this survey indicated that most of the respondents agreed or are willing to accept biometric authentication technology to be used as security on mobile devices. However, further research needs to be conducted in this area.

References

Abdaulwahid, A. A. (2016). Continuous and transparent multimodal authentication: Reviewing the state of the art. *Cluster Computing,* 79**,** 105.

Abraham, J., & Barker, K. (2014). Exploring gender difference in motivation, engagement and enrolment behaviour of senior secondary physics students in New South Wales. *Research in Science Education,* 45**,** 59–73.

Adam, H. (2019). Research sampling and sampling size. *Computers and Eductaion* 4**,** 1223-1224.

Ajzen, I., & Fishbein, M. (1980). *Understanding attitude and predicting social behaviour*. Engelwood Cliffs. NJ: Prentice- Hall.

Akyuz, D. (2018). Measuring technological pedagogical content knowledge (TPACK through performance assessment. *Computers & Education,* 125**,** 212-225.

Albrecht, A. (2003). The biometric industry report. *Market and Technology Forensic to 2003***,** 4, 59-79.

Allan, A. (2003). Biometric authentication: Perspective. *Gartner Research***,** 1-31.

Ang, M. C., Ramayah, T., & Amin, H. (2015). A theory of planned behaviour perspective on hiring Malaysians with disabilities. *Equality, Diversity and Inclusion*: *An International Journal,* 34**,** 186-200.

Anil, K., & Jain, S. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters,* 70**,** 105.

Asha, S., & Chellapan, C (2012). Biometrics: An overview of the technology issues and applications. *International Journal of Computer Applications,* 39, 45.

Ashbourn, J. (2004). Where we really are with Biometrics'. *Biometric Technology Today*, 12**,** 7-9.

Asiimwe, E. N., & Orebro, A. (2015). MLCMS actual use, perceived use and experiences of use. *International Journal of Education Development using Information and Communication Technology,* 11**,** 102-121.

Babbie, E. R. (2010). *The practice of social research*, Cengage Learning.

Bagozzi, R. P., Davis, F.D., & Warshaw, P.R. (1992). Development and test of a theory of technological learning and usage. *Human Relations,* 45**,** 660-686.

Bao, P., Pierce, J., Whittaker, S., & Zhai, S. (2011)-a. Smartphone use by non-mobile business users. In MobileHCI, Stockholm, Sweden. Attitudes and Practices. *Computers & Security*, 24**,** 519-527.

Barbara, A., Belanger, F., & Schaupp, L.C. (2017). Online communities: Satisfaction and continued use intention. *Researcher Pository*, 22.

Benbasat, I., & Barki, H. (2007). Quo vadis, TAM? *Journal of the Association for Information Systems*, 8**,** 211.

Bernard, H. R. (2011). *Research methods in anthropology*, Altamira Press.

Berryman., D. R. (2019). Ontology, epistemology, methodology and methods: Information for librarian researchers. *Medical Reference Services Quaterly,* 38**,** 271-279.

Bhagavatula, R. (2015). Biometric authentication on iPhone and Android: Usability, perceptions, and influences on adoption Research Collection School of Information Systems.

Bhargava, A., & Ochawar, R.S. (2013). Biometric in access control. *International Journal of Emerging and Advanced Engineering,* 3 (4), 11-14.

Biometrics. (2020). Biometrics: definition, trends, use cases, laws and latest news.

Blaikie, N. (2007). *Approaches to social inquiry*. Cambridge.

Brown, S. A., Massey, A.P., Montoya-Weiss, M.M., & Burkman, J.R. (2002). Do I really have to? User acceptance of mandated technology. *EUR J Inform Syst R,* 11**,** 283-95.

Barrios, B. L. (2019). The impact of poor oral health on the oral health-related quality of life (OHRQoL) in older adults: The oral health status through a latent class analysis. *BMC Oral Health,* 19**,** 141.

Bryman, A. (2012). Social research methods, Oxford University Press.

Brymand, A. (2006). Integrating quantitative and qualitative research: How is it done? *SAGE Journals,* 6, 97-113.

Burt, C. (2020). Digital identity predictions for 2020: Biometrics, deepfakes, cybersecurity and decentralized ID [Online]. Available: https://www.fintechnews.org/digital-identity-predictions-for-2020/ [Accessed 27 October 2020].

Burtescu, E. (2010). Reliability and security = convergence or divergence. *Informatica Economica,* 14 (4), 68-77.

Burton-Jones, A., & Hubona, G.S. (2006). The mediation of external variables in the technology acceptance model. *Info. & Mgt.,* 44**,** 706-717.

Cadete, L. (2017). What is a pilot study [Online]. Available: https://s4be.cochrane.org/blog/2017/07/31/pilot-studies/ [Accessed 19 September 2020].

Capps, R. (2019). *The biometric trust* [Online]. Available: https://www.biometricupdate.com/201906/the-biometric-trust [Accessed 27 October 2020].

Carr, L. (2009). The strength and weaknesses of quantitative and qualitative research: What method for nursing? . *Journal of Advanced Nursing,* 4**,** 716-721.

Chao, C. (2019). Factors determining the behavioural intention to use mobile learning: An application and extension of the UTAUT model. *Frontiers in Psychology,* 10.

Chau A., Stephen. G., & Jamieson R. (2004). Biometrics acceptance-perception of use of biometrics. *Association for Information Systems* (ACIS), Proceedings. 28.

Chau, P. Y. K., & Hu, P.J.H. (2002). Examining a model of information technology acceptance by individual professionals: An exploratory study. *Journal of Management Science and Information Systems,* 18**,** 191-229.

Chen, C. L., Lee, C.P., & Hsu, C.Y. (2012). Mobile device integration of a fingerprint biometric remote authentication scheme. . *International Journal of Communication Systems.,* 25**,** 585-597.

Cheng, X., Fu, S., Sun, J., Bilgihan, A., & Okumus, F. (2019). An investigation on online reviews in sharing economy driven hospitality platforms: A trust. *Tourism Management,* 71**,** 366-377

Chesney, T. (2006). An acceptance model for useful and fun information systems. *An Interdisciplinary Journal on Humans in ICT Environments,* 2**,** 225-235.

Cho, D. (2006). Pupil and iris localization for iris recognition in mobile phones. *In Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing.*

Clarke, N., & Furnell, S. (2005). Authentication of users on mobile telephones- a survey of attitudes and practices, *Computer & Security*, 24 (7), 519-527.

Clarke, N. L., & Furnell, S.M (2007). Advanced user authentication for mobile devices. *Computers & Security.*, 26**,** 109-119.

Clarke, N. L., Furnell, S., Rodwell, P. M. & Reynolds, P. L., (2002). Acceptance of authentication methods for mobile telephony devices. *Computers & Security*, 21**,** 220-228.

Collis, J., & Hussey, R. (2003). Business research: A practical guide for undergraduate and postgraduate students., Basingstoke, Palgrave Macmillan:Camden.

Committee, W. B. (2010). Biometric recognition: Challenges and opportunities. *National Academies Press.* Washington.

Corbin, J. A. (2008). *Basics of qualitative research,* London, SAGE Publications, Inc. https://doi.org/10.4135/9781452230153.

Corcoran, P., & Costache, C. (2016). Smartphones, biometrics, and a brave new world. *IEEE Technology And Society Magazine,* 35 (3), 59-66.

Corry, M., Porter, S., & Mckenna, H. (2018). The redundancy of positivism as a paradigm for nursing research. *Nursing Philosophy*, 20 (1).

Creswell, J. W. (2005). *Qualitative, quantitative and mixed methods approaches*. SAGE Publications.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative and mixed methods approaches*. Sage Publications.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use and user acceptance of information technology. *MIS Quaterly,* 13**,** 319-39.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science,* 35**,** 982-1003.

De Luca, A., Hang, A., Zezschwits, E., & Hussmann, H. (2015). I feel like I am taking selfies all day. *The 33rd Annual ACM conference.* Seoul, Korea.

De Vaus, D. A. (2002). *Survey in social research. 5th ed,* Australia, Allen and Unwin.

Deane, F., Barelle., K., Henderson, R. & Mahar, D. (1995). Perceived acceptability of biometric security systems. *Computers & Security,* 14**,** 225-231.

Denzin, N. L. (2002). The qualitative inquiry reader. London: Sage Publications.

Dillion, A., & Morris, M. (1996). User acceptance of information technology: Theories and models. *Annual Review of Information Science and Technology* 31**,** 3-32.

Driscoll, D., Yeboah, A., Salib, P., & Rupert, D. (2017). Merging qualitative and quantitative data in mixed methods research: How to and why not. *International Journal of Computer and Information Technology*, 2**,** 111-114.

Emily, M., Johnson, A.H.I.P., & Carmen, H. (2019). A library mobile device deployment to enhance the medical student experience in a rural longitudinal integrated clerkship. *Journal of the Medical Library Association,* 7**,** 1558-9439.

Fathema, N., & Sutton, K. (2014). Factors influencing faculty members' learning management systems adoption behavior: An analysis using the Technology Acceptance Model. *International Journal of Trends in Economics, Management & Technology,* 2**,** 20-28.

Fathema, N., Shannon, D., & Ross, M. (2015). Expanding the Technology Acceptance Model (TAM) to examine faculty use of Learning Management Systems (LMS). *Journal of Online Learning and Teaching,* 11**,** 210-233.

Fathy, M. E., Patel, V. M., & Chellappa, R. (2015). Face-based active authentication on mobile devices. In Acoustics, speech and signal processing (icassp). *2015 IEEE International Conference on Economics, Business and Management***,** 1687–1691.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behaviour: An introduction to theory and research*. Reading, MA: Addision-Wesley.

Fraenkel, J. R., Wallen, N.E., & Hyun, H.H. (2012). *How to design and evaluate research in education.* New York: McGraw-Hill.

Frucci, M., Galdi, C., Nappi, M., Riccio, D., & Sanniti Di Baja, G. (2014). Iris detection on mobile devices. *In pattern recognition***,** 1752-1757.

Furnell, S. M., Dowland, P. S., Illingworth, H. M. & Reynolds, P. L. (2000). Authentication and Supervision: A Survey of User Attitudes. *Computers & Security.,* 19**,** 529-539.

Gao, Q., Rau, P.P., & Salvendy, G. (2009). Perception of interactivity: Effects of four key variables in mobile advertising. *International Journal of Human Computer Interaction,* 25**,** 479.

Gay, L. R., Mills, G.E., Airasian, P. (2009). Educational research competencies for applications.*Open Access Library Journal,* 2 (5).

George, D., Mallery, P. (2006). SPSS for windows step by step: A simple guide and reference., Boston, Allyn and Bacon.

Giesing, I. (2003). User Perceptions Related to Identification Through Biometrics within Electronic Business. [Online]. University of Pretoria. Available: http://upetd.up.ac.za/thesis/available/etd-01092004-141637/ [Accessed 17 February 2020].

Giesing, I. (2020). User Perceptions Related to Identification Through Biometrics within Electronic Business. University of Pretoria [Online]. Available: http://upetd.up.ac.za/thesis/available/etd-01092004-141637/ [Accessed 17 February 2020].

Gilbert, N. (2001). The importance of pilot studies. *Social Research Update,* 35.

Gliem, A. J., & Gliem, R.R. (2003). Calculating, interpreting, and reporting Cronbach's Alpha reliability coefficient for Likert-type scales. *Research to Practice Conference in Adult, Continuing, and Community Education.* Midwest, Ohoi State University: Columbus.

Goddard, W., & Melville, S. (2004). *Research methodology: An introduction*. Blackwell Publishing.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report,* 8 (4), 597-607.

Griethuijseng, R. A., Eijck, L.F., Haste, H., Brok, P.J., Skinner, N.C., & Mansour, N. (2014). Global patterns in students' views of science and interest in science. *Research in Science Education,* 45**,** 581-603.

Gulati, P. M. (2009). *Research management: Fundamental and applied research*. Global India Publications, India: New Delhi.

Gunther, M., Shafey, L., & Marcel, S. (2016). Face recognition in challenging environments: An experimental and reproducible research survey. *Computer Science, Psychology***,** 247-280.

Gutkowski, P. (2004). Algorithm for retrieval and verification of personal identity using bimodal biometrics. *Information Fusion,* 5**,** 65-71.

Gunarto, L., & Harry, S. (2019). *Pa*rametric & Nonparametric Data Analysis for Social Research: [Online]. IBM SPSS: LAP Academic Publishing. Available: https://www.amazon.com/dp/2100118728.ISBN978-6200118728 [Accessed 19 September 2020 2020].

Hair, J. F., Hult, G.T., Ringle, M., & Sarstedt, M. (2014). A primer o partial least squares structural equational modelling (PLS-SEM). Los Angeles, CA: Sage Publications.

Haq, M. (2014). A comparative analysis of qualitative and quantitative research methods and a justification for adopting mixed methods in social research. *Annual PhD Conference*, University of Bradford Business School of Management.

Harris, A. J., & Yen, D.C. (2002). Biometric authentication: Assuring access to information. *Information Management and Computer Security.,* 10**,** 12-19.

Heerink., M., Krose, B., Evers, V., & Wielinga, B. (2010). Relating conversational expressiveness to social presence and acceptance of an assists social robot. *Visual Reality,* 14**,** 77-84.

Ho, G., Stephens, G., & Jamieson, R (2003). Biometric Authentication Adoption Issues. *Proceedings of the 14th Australasian Conference on Information 2003.*

Holden, R. J., & Karsh, B.A. (2009). Theoretical model of health information technology usage behaviour with implications for patient safety. *Behav Inf Technolo,* 28**,** 21-38.

Horton, R. P., Buck, T., Waterson, P.E., & Clegg, C.W. (2013). Explaining technology acceptance model. *Journal of Information Technology,* 16**,** 49-237.

Hu, P. J., Chau, P. Y. K., & Sheng, O. R. L. (1999). Examining the tehnology acceptance model using physician acceptance of telemedicine technology. *Journal of Management Information Systems,* 16**,** 91-112.

Jain, A., Ross, A., & Nandakumark, K. (2011). Biometric template security. *Adv. Signal Process,* 13 (1), 4-20.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEE Transactions on Circuits and Systems for Video Technology,* 13 (1), 4-20

James, T., Pirim, T., Boswell, K., Reithel, B., & Barkhi, R. (2017). Determining the intention to use biometric devices: An application and extension of the technology acceptance Model. *Journal of Organizational and End User Computing*, 18 (2), 1-25.

Javidnia, H. (2016). Palmprint as a smartphone biometric. *In Proc. IEEE Int. Conf. Consumer Electronics (ICCE).*

Jankowski, R. K., Flannelley, K.J., & Flannelley, L.T. (2018). Threats to internal validity of experimental and quasi-experimental research in health care. *Journal of medicine,* 24**,** 107-130.

Jebreen, I. (2012). Using inductive approach as research strategy in requirements engineering. *International Journal of Computer and Information Technology,* 1**,** 162-173.

Jeong, S. K. (2005). Iris recognition in mobile phone based on adaptive gabor filter. *International Conference on Biometrics*, 3832, 457-463.

Jo, Y. H. (2016). Security analysis and improvement of fingerprint authentication for smart phones. *Mobile Information System*, 2016, 1-11

Jordan, G., Leskovar, R., & Maric, M. (2018). Impact of fear of identity theft and perceived risk on online purchase intention. *Organizacija*, 51 (2), 146-155.

Kadena, E., & Ruiz, L. (2018). Adoption of biometrics in mobile devices. *Springer*.140-148

Karnan, M. (2011). Biometric personal authentication using keystroke dynamics: A review. *Applied Soft Computing,* 11**,** 1565-1573.

Kasinski, A. L. (2008). Inhibition of IkappaB kinase-nuclear-factor-kappaB signal pathways. *Journal of Medicine,* 7**,** 77-99.

Kauber, A., A. (2011) What's wrong with science of MIS. *Honolulu, Proceedings of the 2011,* Decision Science Institute.

Kaur, D., & Savedna, G. (2013). Multimodal biometrics at feature level fusion using texture features. *International Journal of Biometrics and Bioinformatics*, 7**,** 58-73.

Kelly, K., Clark, B., Brown, V., & Sitzia, J. (2003). Good practice in the conduct and reporting of survey research. *International Journal or Quality in Health Care,* 15, 261-266.

Kim, B. (2010). An empirical investigation of mobile data service continuance: Incorporating the theory of planned behaviour into the expectation–confirmation model. *Expert Systems with Applications,* 37**,** 7033-7039.

Kim, D. J., & Hong, K.S. (2008). Multimodal biometric authentication using teeth image and voice in mobile environment. *IEEE Transactions on Consumer Electronics,* 54 (4).

Kim, D. J., Chung, K.W., & Hong, K.S. (2010)-b. Person authentication using face, teeth and voice modalities for mobile device security. *IEEE Transactions on Consumer Electronics*, 54 (4).

Kim, J. S., Li, G., Son, J., & Kim, J. (2015). An empirical study of palm print recognition for mobile phones. *IEEE Transactions on Consumer Electronics*, 53 (6), 593-597.

Kljunic, J., & Vukovac, D.P. (2015). A Survey on Usage of Mobile Devices for Learning among Tertiary Students in Croatia. *Central European Conference on Information and Intelligence Systems.*

Knafl, G. J., & Grey, M. (2007). Factor analysis model evaluation through likelihood cross-validation. *Statistical Methods in Medical Research,* 16**,** 77-102.

Kolacz, H. (2002). *Statistics 252: Multiple regression [*Online]. Available: http://www.stat.ualberta.ca/~kolacz/sta t252/childmupage.html. [Accessed 10 October 2020].

Kong, A. (2009). A survey of palmprint recognition. *Pattern Recognition*, 42**,** 1408–1418.

Kong, W. K., Zhang, D. & Li, W. (2003). Palmprint feature extraction using 2-D Gabor Filters. *Pattern Recognition,* 36**,** 2339-234.

Kothari, C. B. (2012). *Research methodology: An introduction. In Research Methodology: Methods and Techniques*. New Age International (P) Publishers. Daryaganj: New Delhi.

Kurkovsky, S. (2010). Experiments with simple iris recognition for mobile phones. *Proceedings of the 2010 Seventh International Conference on Information Technology*, 1293-1294.

Kyrezis, N. (2010). Linking trust to use intention for technology-enabled bank channels: The role of trusting intentions. *Psychology & Marketing,* 7**,** 799-820.

Lakshman, V. (2018). *The future of biometric authentication lies beyond mobile apps*. Available: https://www.biometricupdate.com/201812/the-future-of-biometric-authentications-lies-beyond-mobile-apps. [Accessed 10 October 2020].

Lankton, K.N., McKnight., D.H., & Tripp, J. (2015). Technology, humanness and trust: Rethinking trust in technology. *Journal of the Association for Information Systems*, 16 (10), 880-918.

Lee, H. C., Park, K.R., Kang, B.J., & Park, S.J. (2009) A new mobile multimodal biometric device integrating finger vein and fingerprint recognition. Proceedings of the 4th International Conference on Ubiquitous Information Technologies and Applications.

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

Lerner, S. (2019). *Mobile security best practices*. Available: https://www.Mobile Security Best Practices|Are You Protecting Your Mobile Devices? (globallearningsystems.com). [Accessed 15 October 2020].

Li, J. (2020). Blockchain technology adoption: Examining the Fundamental Drivers. Proceedings of the 2nd International Conference on Management Science and Industrial Engineering, ACM Publication, 253-260.

Liao, S., Hong, J.C., Wen, M.H., Pan, Y.C., & Wu, Y.N. (2018). Applying Technology Acceptance Model (TAM) to explore Users' Behavioural Intention to Adopt a Performance Assessment System for E-book Production. *EURASIA Journal of Mathematics*, 14 (10), 2-12.

Lindsay, S., Sultany, A., & Reader, K. (2010). An investigation into student mobile devices at City University, London: Evaluating the potential for mobile learning. London: Learning Development Centre and the Schools of Arts and Social Sciences.

Lodico, M. G., Spaulding, D.T., & Voegtle, K.H. (2010). *Methods in education research: From theory to practice*. Jossey-Bass: San Francisco.

Lopez-Nicolas, C., Molina-Castillo, F. J., & Bouwman, H. (2008). An assessment of advanced mobile services acceptance: Contributions from TAM and diffusion theory models. *Information & Management,* 45, 359-364.

Lowry, B. P., Gaskin, J., Twyman, N.W., Roberts, T.L., & Bryan, I. (2013). Taking fun and games seriously: Proposing the hedonicmotivation system adoption model (HMSAM). *Journal of the Association for Information Systems,* 14**,** 617-671.

Lunceford, B. (2009). Reconsidering technology adoption and resistance: Observations of a Semi-Luddite. *Explorations in Media Ecology,* 8**,** 29-47.

Mac Callum, K., Jeffrey, L.M., & Kinshuk, N.A. (2014). Factors impacting teachers' adoption of mobile learning. *Journal of information technology education,* 13, 142-162.

Marsico, M. D., Nappi,M., Narducci, F & Proenc, H. (2018). Insights into the results of MICHE I - Mobile Iris CHallenge Evaluation. . *Pattern Recognition,* 74**,** 286-304.

Maruping, L. M., Bala, H., Venkatesh, V., & Brown, S.A. (2016). Going beyond intention: Intergrating behavioural integration into the unified theory of acceptance and use of technology. *Journal of the Association for Information Science and Technology,* 68 (3), 623-637 .

Matsunaga, M. (2010). How to factor-analyse your data right: Do's, don'ts, and how-to's. *International Journal of Psychological Research,* 3**,** 97-110.

Meriwether, N. (2001). *12 easy steps to successful research papers*, Lincolnwood IL: National Textbook Co.

Mohamed, W. N., Shaari, A.J., Ismail, Z., & Anuar, Y.M.S. (2018). Instructors' behavioural intention towards mobile technology device acceptance. *Advanced Science Letters*, 24**,** 2532-2535.

Monrose, F., & Rubin, A.D. (2000). Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems.*, 16**,** 351-359.

Moon, J., & Kim, Y. (2001). Extending the TAM for a world-wide-web context. *Information and Management*, 38**,** 217-230.

Nadri, H., Rahimi, B., Loft, N.A., Mahnaz, S., Garavand, A., & Hadi, I.(2018). Factors Affecting Acceptance of Hospital Information Systems Based on Etended Technology Acceptance Model. A case Study in Three Paraclinical Departments. *Applied Clinical Informatics*, 9 (6), 112-119.

Neal, D. L., & Woodward, D.L.T. (2016). Surveying biometric authentication for mobile device security. *Journal of Pattern Recognition Research*, 3 (4), 10-18.

Newcastle. (2019). Introduction to Qualitative Research Methods (Inactive*)* [Online]. Available: https://www.ncl.ac.uk/postgraduate/modules/HSC8051 [Accessed 19 September 2020 2020].

Newspoll (2012). Rite aid deployed facial system in hundreds of Australia public. *Journal of Organizational and End User Computing*, 4**,** 110-115.

Nursiah, M. (2020). The effect of computer self-efficacy and subjective norm on the perceived usefulness, perceived ease of use and behavioural intention to use technology. *Journal of Southeast Asian Research*, 2020 (2020)**,** 1-11.

Oishi, J., Kurokura, S.M., & Yegi, P. (2019). Combining observations from multiple platforms across the Kuroshio Northeast of Luzon: A highlight on PIES data. *Journal of Atmospheric and Oceanic Technology,* 33**,** 2185-2203.

Okafor, D. J., Nico, M., & Azman, B. B. (2016). The influence of perceived ease of use and perceived usefulness on the intention to use suggested online advertising workflow. *Canadian Journal of Science and Technology,* 6 (14), 162-174.

Ouedraogo, S. (2020). Estimation of older adult mortality from imperfect data: A comparative review of methods using Burkina Faso censuses. *A Peer-reviewed, Open-access Journal of Population Sciences,* 43**,** 1119-1154.

Pallant, J. (2011). *Multivariate analysis of variance. SPSS survival manual*. Crows Nest: Allen & Unwin.

Parveen, F., & Sulaiman, A. (2008). Technology complexity, personal innovativeness and intention to use wireless internet using mobile devices in Malaysia. *International Review of Research Papers,* 4**,** 1-10.

Pedhazur, E. J. (2016). *Multiple regression in behavioural research,* Fort Wort, TX: Harcourt Brace.

Pelissier, R. (2008). *Business research made easy*. Juta & Co: Cape Town.

Pett, M., Lackey, N., & Sullivan, J. (2003). *Making sense of factor analysis*. Thousand Oaks*:* Sage Publications.

Petters, J. (2020). Data privacy guide: Definitions, explanations and legislation. *International Journal of Data Sciences,* 3, 223-224.

Pikkarainen, T., Pikkarainen, K., & Karjaluoto, H. (2004). "Consumer acceptance of online banking: An extension of the Technology Acceptance Model. *Internet Research Electronic Networking Applications and Policy*, 14**,** 224-235.

Prabhakar, P., & Pankanti, S. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security and Privacy Magazine.* 1 (2), 33-42.

Qualcomm. (2018*). Challenges of mobile biometrics.* [Online]. Available: https://www.qualcomm.com/invention/research/projects/deeplearning [Accessed].

Raja, B. K., Raghavendra, R., & Busch, C. (2015). Improving Cross-Smartphone Periocular Verification in Visible Spectrum Using Time-Frequency Features of Laplacian Decomposition. *2015 11th International Conference on Signal-Image Technology & Internet-Based System.*

Ramos, F. L., Ferreira, B.J., Freitas, A.S., & Rodrigues, J.W. (2018). The effect of trust in the intention to use m-banking. *Scientific Periodicals Electronic Libra,* 15 (2), 175-191.

Rattani, A., Reddy, N., & Derakhshani, R. (2018). Convolutional neural networks for gender prediction from smartphone-based ocular images. *IET Biometrics*, 7 (5), 423-430

Reba, K., Birhane, W.B., & Gutema, H. (2019). Validity and reliability of the Amharic Version of the World Health Organization's Quality of Life Questionnaire (WHOQOL-BREF) in patients with diagnosed type 2 Diabetes in Felege Hiwot Referral Hospital, Ethopia. *Journal of Diabetes Research*, 2019**,** 1-7.

Reddy, A., Rattani, A., & Derakhshani, D. (2016). A robust scheme for iris segmentation in mobile environment. *2016 IEEE Symposium on Technologies for Homeland Security*.

Saini, B. (2016). Keystroke dynamics for mobile phones: A survey. *Indian Journal of Science and Technology*, 9 (6).

Samuels, P. (2016). *Advice on exploratory factor analysis*. Centre for Academic Success: Birmingham City.

Sanchez-Franco, M. J. (2010). WebCT-The quasimoderating effect of perceived affective quality on an extending Technology Acceptance Model. *Computers & Education*, 54**,** 37-46.

Saunders, M., & Tosey P. (2015). *Handbook of research methods on human resource development*. Northampton: Edward Elgar Publishing.

Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research methods for business studies.* Harlow: Pearson Education.

Saunders, M., Lewis, P., & Thornhill, A. (2012). *Research methods for business students*. 6th ed. England: Pearson Education.

Saunders, M., Tosey P. (2013) *The Layers of Research Design* [Online]. Available: http://epubs.surrey.ac.uk/806001/ [Accessed 19 September 2020 2020].

Scherer M. J. (2005). *Living in the state of stuck.* 4th ed. Cambridge MA: Brookline Books.

Schumacker, R. E., & Lomax, R.G. (2004). *A beginner's guide to structural equation modelling.* New Jersey: Lawrence Erlbaum.

Sedwick, P. (2012). *External and internal validity in clinical trials*. London: BMJ Publishers.

Sedgwick, P. (2016). *Pearson's correlation coefficient*. London: BMJ Publishers.

Shan, Y., & King, K. W. 2015. The effects of interpersonal tie strength and subjective norms on consumers' brand-related eWOM referral intentions. *Journal of Interactive Advertising*, 15**,** 16-27.

Shanab, E. A., & Talafha, H. (2015). Internet banking adoption in Jordan: The serqual extension. *14th International conference WWW/internet 2015.*

Silverman, D. (2010). *Qualitative research*. London: SAGE Publications.

Sobh, R., & Perry, C. (2006). Research design and data analysis in realism research. *European Journal of Marketing,* 40**,** 1194-1209.

Soiferman, K. L. (2010). *Compare and contract inductive and deductive research approaches.* Manitoba: University of Manitoba.

Spreeuwers, L. J., Hendrikse, A.J., & Gerritsen, K.J. (2012) Evaluation of automic face recognition for automic border on actual data recorded by travellers at Schipol Airport. *Proceedings of the international conference of biometrics special interest group*, 1-6.

Stock, R. M., & Merkle, M. (2018) Can humanoid service robots perform better than service employees? A comparison of innovative behaviour cues. *Proceedings of the 51th Hawaii Giinther International Conference on System Sciences.* 1056-1063.

Tabachnick, B. G., & Fidell L.S., (2005). *Using multivariate statistics*. Boston: Allyn & Bacon.

Tabachnick, B. G., & Fidell, L.S (2007). *Using multivariate statistic*s. Boston: Pearson Education.

Taber, K. S. (2017). The use of Chronbach's Alpha when developing and reporting research instruments in Science Education. *Springer,* 48**,** 1273-1296.

Taherdoost, H., & Masrom, M. (2009). An examination of smart card technology acceptance using adoption model. *ITI 2009 31st Conf. On Information Technology Interfaces***,** 329-334.

Taherdoost, H., & Sahibuddin, S. (2015). How security issues can influence on usage of Electronic Service. *Advanced in Information Science and Computer Engineering***,** 310-316.

Taherdoost, H. (2016). Sampling methods in research methodology; How to choose a sampling technique for research. *International Journal of Academic Research in Management (IJARM),* 5**,** 18-27.

Taherdoost, H., Hamta, G., Ahoora, G., Club, R., Hamta, A., & Tablokar, C. (2019). Importance of technology acceptance assessment for successful implementation and development of new technologies. *Global Journal of Engineering Sciences,* 1 (3), 1-3.

Taherdoost, H., Jalaliyoon, N., Namayandeh, M., Forghani, A., & Zamani, M. (2010). Adoption framework expansion based on the computer ethics' related research models and ethical scenario analysis. *International Conference on Economics, Business and Management,* 2**,** 219-223.

Taherdoost, H., Sahibuddin, S., & Jalaliyoon, N. (2012). Smart Card Security. *Technology and Adoption International Journal of Security*, 5 (2), 74-84.

Tan, G. W., Ooi, K.B., & Phusavat, K. (2012). Determinants of mobile learning adoption: An emperical analysis. *Journal of Computer Information Systems,* 52 (3)**,** 82-91.

Tao, Q., & Veldhuis, R. (2010). Biometric authentication system on mobile personal devices. *IEEE Transactions on Instrumentation and Measurement*, 59 (4), 763-773.

Taylor, S., & Todd, P. (1995). Assessing IT usage: A test of competing models. *Information Systems Research*, 6 (2), 242-256.

Thabane, L., Ma, J., Chu, R., Cheng, J., Ismaila, A., Rois, L.P., Robson, R., Thabane, M., Giangregorio, L., & Goldsmith, G.H., (2010). A tutorial on pilot Studies: The what, why and how. *BMC Medical Research Methodology*, 10 (1), 1-10.

Theng, Y., Sharma, R., & Tan, P.J.S. (2009). Effective e-commerce strategies for small online retailers. *International Journal of Electronic Business*, 7**,** 445-472.

Toledano, T. D., Pozo, R.F., Trapote, A.H., & Gomez H.L. (2006). Usability evaluation of multimodal biometric verification systems. 18**,** 1001-1122.

Tullis, T. S., & Stetson J.N. (2004). A comparison questionnaire for accessing website usability. *Human Interface Design*, 4, 1-13.

Turner, M., Kitchenham, B., Brereton, P., Charters, S., & Budgen, D. (2010). Does the technology acceptance model predict actual use? A systematic literature review. *Information Software Technologies*, 52**,** 79-463.

Tuunainen, V. K., Pitkanen, O., & Hovi, M. (2009). Users' awareness of privacy on online social networking sites. *Bled 2009 Proceedings*, 42.

Unisys. (2012). Unisys security index report Australia: Facial recognition [Online]. Available: http://www.unisyssecurityindex.com/system/resources/uploads/101/original/Australian2012.pdf [Accessed].

Ursavas, E. (2015). A decision support system for Quayside operations in a container terminal. *Decision Support System*, 59, 312-324.

Uyanik, K. G., & Guler, N. (2013). A study on multiple linear regression analysis. *4th International Conference on New Horizons in Education.* Turkey: Sakarya Universitesi.

Van Biljon, J., & Kotze, P. (2008). Cultural factors in a mobile phone adoption and usage model. *Journal of Universal Computer Science*, 14**,** 2650-2679.

Vatcheva, P. V., Lee, M., Mccromick, B.J., Rahbar, M.H. (2016). Multicollinearity in regression analysis conducted in epidemiology studies. *Epistemology*, 6 (2), 227.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and research agenda on interventions. *Decision Sciences,* 39**,** 273-315.

Venkatesh, V., & Davis F.D. (2000). A theoretical extension of technology acceptance model: Four longitudinal field studies. *Management Science*, 46**,** 186-204.

Venkatesh, V., & Davis, F. D. (1989). A model of the antecedents of perceived ease of use: Development and test. *Decision Sciences,* 27**,** 451-481.

Venkatesh, V., Morris, M.G., Davis, G.B., & Davis, F.D. (2003). User acceptance of information technology: Toward unified view. *MIS Quarterly,* 27**,** 425-478.

Vrana, R. (2018). Acceptance of mobile technologies and m-learning in higher education learning: An explorative study at the Faculty of Humanities and Social Science at the University of Zagreb. *Proceedings of* C*roatian Society for Information and Communication Technology, Electronics and Microelectronics*, 814-819.

Vuong, Q. H., & Trang, H.M. (2018). An open database in vitamin's social science and humanities for the public. *IEEE of Transaction of Information Foreignsic and Security,* 5**,** 111-114.

Wang, H., & Liu, J. (2009). Mobile phone-based health care technology. *Recent Patents on Biomedical Engineering*, 2**,** 15-21.

Welman, W., Kruger, F., & Mitchell, B. (2015) *Research methodology*. 3rd ed. Cape Town: Oxford University Press.

Weng, F., Yang, R.J., Ho, H.J., & Su, H.M. (2019). A TAM based study of the attitude towards use intention of multimedia among school teachers. *Applied System Innovation,* 1 (36), 1-9.

Wilson, J. (2010). *Essentials of business research: A guide to doing your research project*. 2nd ed. London: SAGE Publications.

Wirtz. (2020). Service Robots & AI-The Service Revolution has Begun-Master Class [Online]. Available: https://www.researchgate.net/publication/341878196 [Accessed 09 August 2020].

Wits. (2019). Publishing, research support, scholarly communication [Online]. Available: https://libguides.wits.ac.za/research-support [Accessed 19 September 2020 2020].

Wojciechowska, M., Chora´s., & Kozik, R. (2017). The overview of trend sand challenges in mobile biometrics. *Journal of Applied Mathematics and Computational Mechanics.,* 16(2), 173-185.

Woodward, D. L., Pundlik, J.S., Lyle, J.R., & Miller, P.E. (2010). Periocular region appearance cues for biometric identification. *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition***,** 8.

Woodard, J. D. (2016). Biometrics: Privacy's Foe or Privacy's Friend? *Proc. IEEE,* 2016, 1480-1492.

Wu, J. (2011). Developing an explorative model for SaaS adoption. *Expert Systems with Applications,* 38**,** 15057-15064.

Wu, J., & Wang, S. (2005). What drives mobile commerce?: An empirical evaluation of the revised technology acceptance model. *Information & Management,* 42**,** 719-729.

Yamazaki, K. (2015). Learning biometrics [Online]. Available: https://theyamazakihome.com/ [Accessed 05 October 2020].

Zeynivandnezhad, F., Rashed, F., & Kaooni, A. (2019). Exploratory factor analysis for TPACK among mathematics Teachers: Why, what and how. *Anatolian Journal of Education*, 4**,** 59-76.

Zydney, J., & Warner, Z. (2016). Mobile apps for science learning: Review of reaserach. *Computers and Education*, 94, 1-17.

Appendix A: Request for conducting research

Request for conducting research

10 May 2020

HOD

Department of Information and Communication Technology

Vanderbijlpark

1911 Andries Potgieter

South Africa

Greetings

I, Malatji William Ratjeana with student number 214005720 and ID number 9210015524081 am doing research under the supervision of Professor Tranos Zuva in the Department of Information and Communication Technology at the Vaal University of Technology. I am doing the research towards fulfilment of requirements for Masters in Information Technology.

I am requesting your permission to conduct a research entitled "Acceptance of biometric authentication security technology on mobile devices". The aim of the research is to find out the perception of acceptance of biometric authentication technology on mobile devices.

The research entails a quantitative non-experimental survey. Participants will citizens in Johannesburg (Vanderbijlpark) South Africa. A survey questionnaire will be used to collect data and will be administered by the researcher.

There is no anticipated risk to the study and participants can withdraw any time if they wish to do so without any obligation. The results of the study will be used for academic purposes only.

Should you require any further information about any aspect of this request or the study, please contact me on 072 556 6139, villywr@gmail.com. My supervisor Prof Tranos Zuva may be contacted on 016 950 7587 or tranosz@vut.ac.za.

Yours sincerely;

Malatji W.R

Signature

Mr, WR Malatji: Student Researcher

I……., the HOD in the Department of Information and Communication Technology hereby give my permission to the student to conduct a research entitled "Acceptance of biometric authentication security technology on mobile devices" and I fully understand the objectives of the study.

…… ……

Signature Date

Appendix B: Informed consent

CONSENT FOR PARTICIPATION IN SURVEY RESEARCH

PLEASE READ THIS DOCUMENT CAREFULLY. YOUR DETAILS ARE REQUIRED FOR PARTICIPATION.

Research title: "Acceptance of biometric authentication security technology on mobile devices"

Researcher's name: William Ratjeana Malatji

Researcher's relationship with VUT: Research Masters Student

Research Supervisor: Prof Tranos Zuva

Research Co-supervisor: Dr Rene Van Eck

MR. William Ratjeana Malatji of the Vaal University of Technology has invited me to participate in a research project. I understand that the study's aim is to collect data on mobile biometrics.

1. I have read the study's information sheet and have had the study's specifics clarified to me.
2. I accept that I will not be compensated for my participation, and that I am free to withdraw and discontinue at any time.
3. I believe that the majority of survey participants would find the questionnaire interesting. I have the right to refuse to answer any question if I am dissatisfied in any way during the survey.
4. I accept that the researcher will not mention me by name in any reports based on survey data, and that my confidentiality as a study participant will be protected.

…… ……

Participant's signature Date

Malatji W.R

.....

Researcher’s Signature

Appendix C: The questionnaire

No.	Construct	Measuring Item	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Source-citations
Q1	Perceived Usefulness	Using the mobile biometric device in my job would enable me to accomplish tasks more quickly	136	113	47	4	2	(Emily, Johnson and Carmen, 2019)
Q2		Using mobile biometric device would improve my job performance.	111	107	75	6	3	
Q3		Using mobile biometric device would enhance my effectiveness on the job.	113	117	64	6	2	
Q4		I would find a mobile biometric device useful in my job and for personal use.	120	110	62	6	4	
Q5	Perceived Ease of Use	My interaction with the mobile biometric device would be clear and understandable.	128	124	44	3	3	(Emily, Johnson and Carmen, 2019)
Q6		I would find a mobile biometric device to be flexible to interact with.	113	115	67	5	2	
Q7		Learning to operate the mobile biometric device would be easy for me.	116	125	50	9	2	
Q8		I would find a mobile biometric device easy to use.	117	115	59	4	7	
Q9	Subjective Norm	People who influence my behaviour think that I should use the mobile biometric device	74	96	58	61	13	(Barbara, Belanger and Schaupa, 2017)
Q10		People who are important to me think that I should use the mobile biometric device.	69	72	94	53	14	
Q11		I use the mobile biometric device because of the proportion of people around me who also do.	67	87	72	59	17	
Q12		People around me who use the mobile biometric devices have more prestige than those who do not	64	76	89	55	18	
Q13	Trust	I do not doubt the honesty of biometric mobile devices	89	92	71	23	27	(Cheng, Sun, Bilgihan and Okumus 2019)
Q14		The mobile biometric device will keep my data private.	76	84	84	32	26	
Q15		The mobile biometric device will keep my data secured.	78	95	74	29	26	
Q16		The mobile biometric device will ensure a reliable security for my device.	74	76	92	33	27	

Q17	Perceived Humanness	I am happy about mobile biometric devices Happy.	100	115	78	4	5	(Lankton, Knight and Tripp, 2015)
Q18		I am satisfied with mobile biometric devices.	68	137	83	9	5	
Q19		I understand mobile biometric devices.	96	118	78	5	5	
Q20	Perceived Interactivity	If I can easily unlock my mobile biometric device without any delay.	131	121	44	5	1	(Gao, Rau and Salvendy, 2009)
Q21		If I will have a lot of control over my mobile biometric device.	94	118	84	5	1	
Q22		If there will better communication between me and my mobile biometric device.	89	117	80	704	2	
Q23	Perceived Social Presence	There is a sense of sociability with mobile biometric devices.	72	129	73	20	8	(Lankton, Knight and Tripp, 2015)
Q24		There is a sense of human warmth with mobile biometric devices.	62	108	83	36	13	
Q25		There is a sense of human contact with mobile biometric devices.	60	129	81	23	9	
Q26	Actual Use of Biometric Mobile Device	I have used the mobile biometric device before.	95	93	63	39	12	(Asiimwe and Orebro, 2015)
Q27		I have used the mobile biometric device for too long.	58	82	76	69	17	
Q28		I often use the mobile biometric device.	63	88	79	57	15	
Q29	Accuracy	I thought there was too much consistency in this mobile biometric device.	105	105	74	8	10	(Tullis and Stetson, 2004)
Q30		I found the various functions in the mobile biometric device well integrated.	86	102	95	11	8	
Q31	Identity Theft	I am afraid that somebody can unlock my mobile biometric device easily.	100	98	64	20	20	(Jordan, Leskovar and Maric, 2018)
Q32		I am very worried that the unauthorised use of my personal data from my mobile biometric device can damage my reputation.	80	101	85	18	18	
Q33	Reliability	I find biometric security, reliable enough to protect my mobile device.	110	91	68	18	15	(Tuunainen, Pitkanen and Hovi, 2009)

Q34	Privacy	I worry about my data privacy While using the mobile biometric device.	113	85	70	20	14	(Tuunainen, Pitkanen and Hovi, 2009)
Q35		I feel that the privacy of my personal information is protected by biometric security on my mobile device.	104	86	91	11	10	
Q36	Security	I worry about my data security while using the mobile biometric device.	106	106	53	18	19	(Tuunainen, Pitkanen and Hovi, 2009)
Q37		I'm familiar with data protection and securing while using mobile biometrics in general.	105	83	95	8	11	
Q38	Identity Assurance	Each user of the mobile biometric device will have unique user traits.	111	116	64	7	4	(Jordan, Leskovar and Maric, 2018)
Q39		The user traits will match my biometric user filed.	93	77	102	24	6	
Q40	Combining Data	I do not have any concern about biometric security responsible for combining my login details on my mobile device	109	112	50	12	19	(Oishi, Kurokura and Yegi, 2019)
Q41	Intention to Use	I intend to use the mobile biometric device in my class or workplace.	146	103	46	6	1	(Weng, Yang, Ho and, 2019)
Q42		I increase the occurrence of using the mobile biometric device in class or workplace.	146	70	77	8	1	