Leiden University

ICT in Business

Consumers' Technology Acceptance of mobile biometric authentication methods for financial transactions

Name:	Dennis Alexander Wansleven
Date:	10/12/2018
1st supervisor:	M.C.A. de Rijk
2nd supervisor:	Prof.dr.S. Jong Kon Chin

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Abstract

In the ever more connected world, with billions of devices and sensors connected to the internet, an increasing number of activities are taking place in the digital realm. As a consequence of this connected world is an increase in the number of transaction fraud and security breaches. Due to their core business, banks and payment service providers are an attractive target for fraudulent activities and the necessity for stronger authentication methods becomes inevitable. Scholars have looked at a variety of possible solutions to these urgent matters and concluded that biometrics might be the solution to fraud and identity theft.

The aim of this study has been to discover the Behavioral Intentions of Dutch consumers regarding biometric authentication methods on mobile devices to authorize financial transactions, and in particular how fingerprint, face, and pattern recognition compare to each other in the eyes of consumers.

Using existing Technology Acceptance theory as a foundation, we proposed a conceptual model incorporating the constructs: Lifestyle Compatibility, Perceived Ease of Use, Perceived Risk, Perceived Privacy Concern, Perceived Security, and Behavioral Intention. Furthermore, based on the different recognition technologies and two different values of the financial transactions (low = 25 Euros; high = 1.0000 Euros) we developed a total of six scenarios which were randomly assigned to respondents of the survey.
After thoroughly testing the survey during multiple iterations with the help of a focus group (N = 15, N = 10, and N = 34) the survey was distributed using social media, email, and messaging applications.

During a period of six weeks, respondents were able to complete this survey. Each respondent (N = 220) was randomly presented with one of the six scenarios followed by questions addressing the aforementioned constructs.

Having performed a Confirmatory Factor Analysis using Structural Equation Modeling, validity and reliability thresholds were met, enabling further analysis. Using multiple linear regression analysis, we were able to test the proposed conceptual model, discovering the significant associations between all constructs in both the first and second model, and in the third model the associations between LC and BI, and between PS and BI.

Resulting from the ANOVA analysis and the post-hoc Tukey HSD test, significant variations among the scenarios were found in all constructs, except Perceived Ease of Use. Overall, using fingerprint recognition technology was perceived as most compatible with the lifestyle of respondents, most secure, least risky and the lowest degree of concern about privacy regarding both low, and high-value transactions.

Concluding from our research it appears that in contrast to fingerprint recognition, face recognition is not yet accepted by the wider public as an authentication method for the authorization of financial transactions. Moreover, pattern recognition (or pattern lock) is found to have the lowest level of security and the highest level of risk. Overall, the executed multiple linear regression analysis indicates that the primary factors contributing to the rejection or acceptance of recognition technologies are the Perceived Lifestyle Compatibility and Perceived Security.

Keywords: TRA, TPB, Technology Acceptance, TAM, DOI, UTAUT, Biometrics, Financial transactions, Fingerprint recognition, Face recognition, Pattern recognition

Acknowledgement

I would like to use this opportunity to express my profound gratitude for all the individuals involved in this thesis or who were part of my journey during the last eight months. While it is impossible to address every single individual who has helped me in any way. The successful completion of this master thesis is a result of your support, advice, input, and guidance. Without all of you, the successful completion of this research project would not have been possible.

First of all, I would like to express my gratitude towards my first supervisor: Tino de Rijk. During the last couple of months his guidance, both face-to-face and through several phone calls, has proven to be invaluable for my personal development and the completion of this thesis. Furthermore, I would like to thank my second supervisor: Prof. dr. Simcha Jong Kon Chin. His valuable insights, remarks, and overall guidance have been a tremendous help to establish this thesis.

Secondly, I would like to express my gratitude to Axel Haenen, who has been my supervisor within Accenture for the last eight months. Our weekly contact proved invaluable to the progress of my thesis and he has been one of the key figures who supported me throughout the entire process and encouraged me to look beyond the horizon. Furthermore, I would like to thank Paul Weiss for his support and input which helped me specify the topic.

Of course, I would also like to thank my family for their support and patience during the exciting moments of the last months. Through the ups and downs they always believed in me and my capabilities, and if necessary, helped me empty my mind. Moreover, all my dearest and closest friends; thank you for dealing with me and all the research related talks. In particular Zennar Ibrahim, my sincere appreciation for your patience, a listening ear, critical thinking, and all the help you offered me during these months. I cannot thank you enough for everything you did.

“*Once you stop learning, you start dying. - Albert Einstein*”

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

Mobile devices have influenced the lives of billions of individuals to an unprecedented degree. Where the first mobile phones were received with criticism, they eventually found their way into our daily lives resulting in billions of mobile phones on the planet. While older technologies took dozens of years to be adopted and accepted by the general public, the adoption of the internet and smartphones has occurred at the fastest rate of any consumer technology so far. [94] As a result of these technological innovations, the financial services industry, and in particular, the retail banking sector has experienced significant changes. The way in which the services are offered to (potential) customers has changed and evolved towards technology-based self-service (Self-Service Technologies or SSTs). Consequently, banking activities nowadays are increasingly performed via electronic channels (e.g. online) and using mobile devices. [106, 71]

It would seem that with such benefits of new technologies and convenience, the adoption of new methods to execute banking activities would not take that long. However, despite the advances in technology, the problem of rejection and under utilization is still present, leading researchers to attempt to discover factors contributing to the acceptance or rejection of technologies. [72]

Driven by these attempts, an extensive body of research has been dedicated to understanding IT acceptance (or Technology Acceptance; TA). [32, 10, 26, 102, 101] Technology Acceptance is a term that is often used interchangeably with other terms referring to whether individuals will either accept or reject a certain technology (e.g. Technology Readiness, Adoption Readiness, and Innovation Adoption). In academia, many researchers have attempted to 'measure' this so-called Technology Acceptance of consumers in relation to a variety of technologies. In our study we are focused on the 'Technology Acceptance' and use the following definition originating from Parasuraman: *"People's propensity to embrace and use new technologies for accomplishing goals in home life and at work. [78, p. 308]"*

The increasing popularity of electronic banking (e-Banking), and in particular mobile banking (mBanking) goes hand-in-hand with a growing cybercrime and fraud threat. As mentioned by Venkatraman: "*As the level of security breaches and transaction frauds increase day by day, the need for highly secure identification and personal verification information systems are becoming extremely important especially in the banking and finance sector. [103]*"

As a result, banks and payment service providers (PSPs) are looking for new, and more secure ways of user authentication. Identity management systems based on biometrics are deemed to be the solution to the security challenges we face today and might be the solution organizations are looking for. [92] Whereas in 2016 the number of mobile payments authenticated by biometrics was 600 million. Research by Juniper Research estimates that this will increase to nearly two billion in 2017. [75]

1.2 Problem statement

In response to the growing cyber threat and the public demand for more convenient ways to log-in and authenticate actions, banks and PSPs are looking at the potential of biometric technologies. As with any other technology, for biometrics to reap its full potential, and for the organization to realize its goals, consumer adoption of the technology is a prerequisite. As history teaches us, however, many technological inventions failed to realize their potential. [37] Thus, a thorough understanding of factors influencing Technology Acceptance could prove essential in the attempt to counter the increasing cyber threats and cases of identity fraud.

In order to address the issue of Technology Acceptance, or *"People's propensity to embrace and use new technologies in order to accomplish their goals in home life and at work."[78, p. 308]* this research aims to obtain an understanding of constructs influencing the TA regarding biometric user authentication for financial transactions.

Despite biometrics being an increasingly accepted technology which enables users to log-in on our mobile devices, the widespread adoption of biometrics to authorize financial transactions appears to be lacking behind.

1.3 Motivation

1.3.1 Theoretical relevance

Research attempting to understand individual acceptance and use of IT is considered as one of the most mature streams of information system (IS) research. [101] As a result, an extensive collection of Technology Acceptance (TA) models has been developed, thoroughly analyzed in subsequent research, and applied to a variety of emerging technologies and innovations. However, previous TA research that applied such models, has mainly focused on the acceptance of: mobile payments (mPayments) [64], mBanking [11, 106] and internet banking (or e-Banking) in general [63, 71, 60] resulting in only few authors conducting research regarding biometric systems from a consumer perspective. [72]

Still, some TA research has focused on biometrics. For example, Miltgen et. al have studied the acceptance of iris recognition in the context of person-bound-services [72], El-Abed et. al have studied the acceptance and satisfaction of biometric systems with a focus on performance, acceptability and satisfaction, security and data quality. [2] Furthermore, Kanak and Sogukpinar developed, and tested, the BioTAM model, building on the Technology Acceptance Model (TAM) by Davis [28] and adding additional constructs (e.g. confidence, and public willingness). Finally, research by Huys aimed to understand the acceptance of biometrics in a physical store. [43] Nevertheless, research regarding biometric authentication using mobile devices (e.g. a smartphone or tablet) appears to be missing. Therefore, our main theoretical contribution is that our study - to the best of our knowledge - is the first and only to consider the TA of biometrics methods supported by mobile devices and in particular a study that compares different technologies and transactions values.

In their study regarding mBanking, Shaikh et. al stated: *"... virtually no studies address the use of mBanking applications via smartphones or tablets or consider the consequences of such usage. [91]"* Our study aims to contribute to this gap by developing scenarios based on mBanking in combination with (biometric) recognition technologies. Moreover, as suggested by Ogbanufe et. al, future research regarding the usage and acceptance of biometrics (i.e. fingerprint) should put the emphasis on both security and privacy aspects. [76] Following the suggestion from Huys, this type of research should be executed in different scenarios, whereas they compared the combination of iris and face recognition with solely fingerprint recognition to execute payments in a grocery store, different scenarios should also be studied. [43] Schierz et. al suggested that future research could adopt their model to ensure its fit to the specific payment solution of the study. [88] Hence, it can be concluded that where previous research has focused on the general acceptance of biometric technologies in other countries [31] and the acceptance of other methods of conducting transactions [41] (e.g. wireless technologies such as NFC or mobile banking in general) [29], a gap regarding the usage of biometric recognition technologies on mobile devices remains.

In view of the existing research regarding the acceptance of m-banking and biometrics, one of the objectives of this study is to empirically test a theoretically grounded conceptual model on biometric user authentication for the authorization of financial transactions. Due to the nature of the banking, and financial sector in general, this conceptual model focuses on security and privacy related constructs in particular. The creation of this model, incorporated variables and hypotheses are discussed in the third part of chapter two.

1.3.2 Practical relevance

This study is conducted in close collaboration with an internationally operating consulting firm located in Amsterdam, The Netherlands. Hence, the practical relevance is focused on three parts: first of all, it contributes to the organization's value proposition. Meaning that the knowledge resulting from this study should contribute to, or improve, the services it provides to its customers and contribute to the organization's understanding of the market.

Second, as many introductions of new technologies appear to face severe difficulties or fail completely, this research should provide insight into the factors contributing to the TA of customers and the potentially beneficial applications of biometric technologies as an authorization method for financial transactions. As mentioned by John Gourville (2006), consumers often attach more value to what they already have (by a factor of three) and executives overvalue their innovations by this same factor, which is called the 'endowment effect'. [37] This study helps to obtain a better, objective, understanding.

Third, the adoption of new technologies is a phenomenon which is difficult to predict. Some markets embraced the introduction of wireless services, while others refused to use them until a later point in time. [13] This study should provide an understanding of customers of bank and payment service providers in The Netherlands, and whether the introduction of biometric-enabled user authentication will be embraced or rejected. Therefore, this research should result in some key factors that contribute to organizational strategic decision making about the implementation of biometric recognition technologies.

1.4 Research questions

Based on the background, problem statement, and previous research the following research question is developed:

"How are consumers of payment services in The Netherlands adopting mobile biometric authentication methods to authorize financial transactions?"

In order to answers the research question, we have formulated the following subquestions:

1. Which factors contributing to consumers' Technology Acceptance are mentioned by previous research?
2. What effect do privacy and security related constructs have on consumers' Technology Acceptance in the case of biometric authentication on mobile devices for the authorization of financial transactions?
3. How does the Technology Acceptance of consumers differ between face recognition, fingerprint recognition and pattern recognition?

4. How does the value of a transaction affect the perception of consumers regarding the usage of different mobile biometric authentication methods for financial transactions?

1.5 Research approach

This study applies the mixed methods approach with the goals to: study what is happening in a certain area, gain insight into a certain topic of interest, and establish and test relations between variables incorporated in a conceptual model. [70]

First of all, a critical literature review has been performed in order to gather and summarize information regarding biometrics, their applications, and theories originating from (TA) and User Adoption literature. Thus, this literature study will provide the answer for the first sub-question of our study, as well as lay the foundation for our conceptual model. The validity of this conceptual model is guaranteed due to its foundation in the research related to its development, previous research to empirically test the model, and research applying these variables. As preliminary searches indicated, the most popular theories and models related to this are: Technology Acceptance Model or 'TAM' as developed by Davis [28] and Unified Theory of Acceptance and Use of Technology abbreviated as 'UTAUT' by Venkatesh [102].

The other sub-questions are answered by empirically testing the conceptual model resulting from the first sub-question. Usin statistical analysis of the constructs included in the conceptual model, conclusions about the associations, effect of the specific technology, and transaction value are formulated.

The main goal of this study is to evaluate consumers' propensity to embrace, and use, biometric technologies as a mobile authentication method for financial transactions and how the technologies and transactions values affect this propensity. Based on previous research and established models which have been thoroughly tested, a new conceptual TA-model has been proposed. By distributing a scenario-based questionnaire we aim to gain an understanding of the relations between constructs of the model, as well as potential differences of Technology Acceptance regarding the biometric authentication method and corresponding purchase value.

1.6 Thesis outline

Concluding this chapter, we provide an overview of the following chapters and their corresponding content.

Chapter 2 discusses the literature review consisting of several key components. We start by providing a brief theoretical background regarding Technology Acceptance (TA) related research, followed by a discussion of biometric traits and current TA-theories and models. Lastly we propose our conceptual model and its corresponding hypotheses.

Chapter 3 discusses the methodology used in the individual phases of this study. First, we describe the process and rationale behind the selection of the biometric trains subject of our study. Secondly, we describe the iterative process (adopted from Design Science Research) applied to the development, testing and validation of the survey. Furthermore, the sample of our survey is illustrated, as well as the design process regarding the scenarios, and the data preparation.

Chapter 4 provides the results of our data gathering phase which will be followed by the discussion of these results in chapter 5. Chapter 6 provides the conclusions and implications (both theoretical as well as practical) and limitations of our research. Concluding our study we also provide some recommendations and suggestions for future research.

Chapter 2

Background and literature review

2.1 Theoretical background

Due to the increasing popularity of Information Technology (IT) and (management) Information Systems (IS), these fields have experienced a lot of attention from academia. Research focused on explaining TA of new technologies (or innovations) is described in the literature as one of the most mature research areas in contemporary IS-literature. [102] Our study builds upon this extensive body of knowledge originating from sociology and psychology and in particular the studies focusing on: Technology Acceptance, innovation adoption, innovation diffusion, and human behavior.

Studies focusing on the obtainment of a better understanding regarding technology adoption often use the same foundation. This foundation is shaped by the work of Ajzen and Fishbein: both their individual papers as well as the papers written in collaboration. Originating from social psychology, Fishbein and Ajzen's Theory of Reasoned Action (TRA) is considered one of the most fundamental and influential theories of human behavior. [9, 102]. In its core, this theory postulates that an individual's intention to perform a specific behavior is the determinant of that action. [7].

Where the TRA focuses on volitional behavior (situations in which they have sufficient control over their behavior) Ajzen's extended model, the Theory of Planned Behavior (TPB) incorporates the additional construct 'perceived behavioral control'. [8, 10] The TPB applies the same assumption as the TRA where an intention to perform (or not perform) a specific behavior is the most important determinant of actually performing that action. However, it applies three basic determinants: one personal, one reflecting the influence of social contacts, and a third one that reflects potential issues with control over the performed intention and/or behavior. [7, 8]

The TRA and TPB have been widely used to increase our understanding of individual adoption behavior as well as explain factors contributing to the adoption of different Information Technologies (IT) and Information Systems (IS). [108, 10, 32] Following the development of these theories and models, a multitude of complementary models have been developed. Davis' Technology Acceptance Model (TAM) [26, 28] was amongst the first models and consequently led to the creation of Venkatesh's Unified Theory of Acceptance and Use of Technology (UTAUT) [102] and subsequently the UTAUT2 [101], which was especially focused on consumers and incorporated additional constructs. At the same time as Davis' TAM, Rogers developed his Diffusion of Innovation Theory (DOI or sometimes referred to as Innovation Diffusion Theory IDT). [85]

2.2 Biometrics

Although the wider public might believe that biometric recognition technologies have only been recently invented, the origins of using unique characteristics for the identification or verification of one's identity dates back to 600 AD. This particular example concerned a document signed by a Chinese merchant using ink and his fingerprint as some kind of signature. [49, 100] In more recent years, and especially since the introduction of fingerprint sensors in smartphones (e.g. the iPhone 5S in 2013), this technology has experienced an increase in popularity and organizations are investigating ways in which they can apply it to improve their security and prevent fraud. [45]

2.2.1 Biometric traits

Biometric recognition refers to the (automated) recognition of an individual based on their anatomical, behavioral of physiological characteristics. [50, 49] However, not all human biological or behavioral characteristics can be used as a biometric identifier. The degree to which a characteristic is suited for automated recognition depends on the degree to which it satisfies the following properties [1, 15, 49, 80, 84]:

1. *Universality*
   The degree to which the biometric trait is present in every individual.
2. *Distinctiveness or uniqueness*
   The biometric trait should be sufficient to distinguish between two or more individuals.
3. *Permanence or stability*
   The degree to which a biometric trait remains unchanged (e.g. resistance to the effect of aging).
4. *Collectability*
   The extent of easiness with which the biometric trait can be measured, collected, or gathered.
5. *Performance*
   Indicates the achievable accuracy, speeds and robustness of the biometric trait.

6. *Acceptability or user acceptance*
   The willingness of individual in the target population to present their biometric trait to a system.
7. *Circumvention*
   The ease with which a biometric trait can be imitated or copied.

Taking these properties in mind, scholars have identified a variety of biometric traits which are presented in figure 2.1 below. Following the illustration, each biometric modality will be discussed briefly.

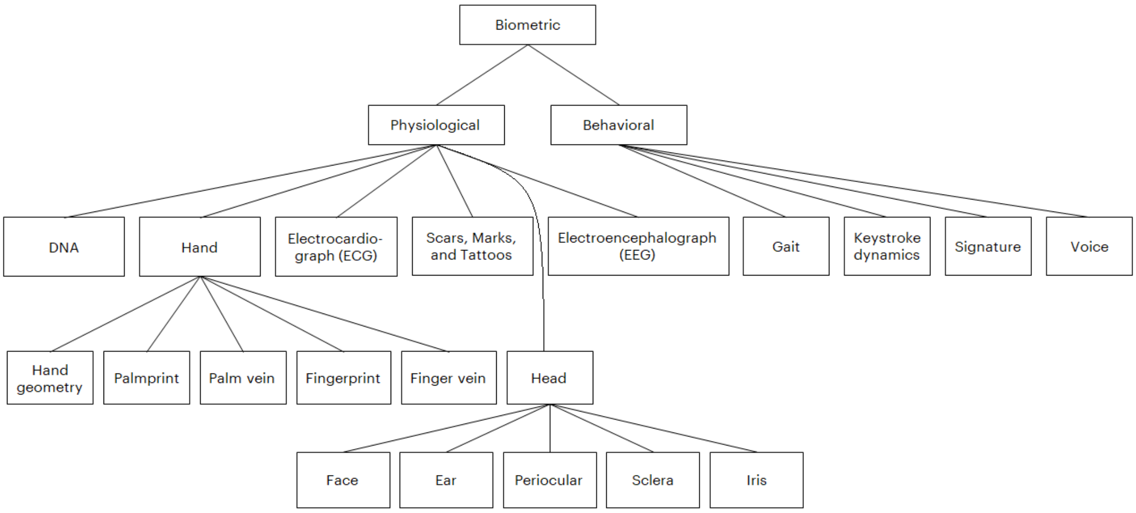


Figure 2.1: Overview of biometric traits [49]

DeoxyriboNucleic Acid (DNA)

DeoxyriboNucleic Acid (DNA) is the chain that includes the blueprint of all living organisms. Known for its helix structure, it contains all the instructions for the growth, development, general functioning and reproduction of humans, fish, plants and all other organisms. This biometric trait is the most unique of all, with the only exception being identical twins. At this moment, this trait is used mostly in forensic identification and of course the field of medicine and biology. [47]

Hand geometry

A quite popular biometric trait is the geometry of our hand. This method measures the 3D-characteristics of our hands by looking at the overall structure, shape and proportions. For example, it measures the length, width and thickness of a hand, the fingers, joints and knuckles. [4] A device is able to scan this because of its optical camera, a variety of mirrors, and LEDs which capture images of the back and sides of the hand. In total, a hand geometry system collects more than 90 dimensional measurements. [83] Scholars have argued that in the case of verification (the check whether a hand print which is presented is the correct one) hand geometry might prove sufficiently distinctive. However, for identification in large populations, hand geometry is not considered to be sufficiently distinctive. [23]

Hand geometry is generally perceived as non-intrusive and non-threatening and lacks the law enforcement association of fingerprint systems association of fingerprint systems. It is considered relatively easy to use by the majority of the population, although some minimal training may be necessary to help the user learn how to align his/her hand accurately in the reader. [83]

Palm print

The human palm print consists of several components which can be used to recognize and differentiate palm prints from one another. Just like human fingerprints, palms contain ridges and valleys that are much larger than the ones present in our fingers, hence this type of recognition requiring a larger scanning device. [23]

To recognize an individual by his or her palm print, the device uses physical features to verify their identity. These features include: principal lines, wrinkles, and ridges present in human palms. [83]

Just like fingerprint recognition, palm print recognition also suffers from excessive dirt, grime or oils and the skin can dirty the platen, which might result in false reads or non-reads. [83]

Palm vein

Palm vein recognition uses vein geometry characteristics which are present in the palms of humans. This type of recognition looks at the full picture of a hand and analyzes the pattern, thickness and location of blood vessels to create a unique template. According to scholars these blood vessels are sufficiently unique to be used for the verification of an individuals' identity. [16]

Palm veins appear to be quite distinctive between individuals and even among identical twins. Research indicates that this technique can be used to successfully verify the identity of an individual. Palm vein recognition uses infrared illumination which gets absorbed or reflected by the hemoglobin in our blood (hemoglobin is a component of the red blood cells which can be found in blood). A big advantage of this technique is the stability of these vessels as we age, however they are susceptible to the effects of declining bone and muscle strength, which is also correlated with some diseases such as diabetes, atherosclerosis or tumors. [74]

Fingerprint recognition

Fingerprint recognition might be one of the oldest biometric traits which are used to identify individuals (e.g. 600AD in China [100]. A fingerprint can be recognized due to a variety of features from which it is built. The first level of features are the macroscopic details such as the ridge flow, ridge frequency, ridge pattern and singular points. The second level features refer to minutiae (e.g. ridge bifurcations and edges). The last level features capture dimensional attributes. [49] As illustrated in figure 2.2 (from left to right): A gray-scale fingerprint image, Level 1 features (orientation field or ridge flow and singular points), Level 2 feature (ridge skeleton and minutiae), and Level 3 features (ridge contour, pore, and dot). [49]

Throughout the years, the context in which it was applied has varied as well as the technology to perform the comparison between a stored- and presented fingerprint. During the first years of the 20th century, the United Kingdom decided to accept fingerprints as evidence for criminal cases. Not much later, in the 1920s, US Congress authorized the Department of Justice to collect fingerprints when a new arrest has been made. Some decades later, in the 1970s, the FBI implemented a new system of comparing fingerprints, the so-called Automated Fingerprint Identification System (AFIS).

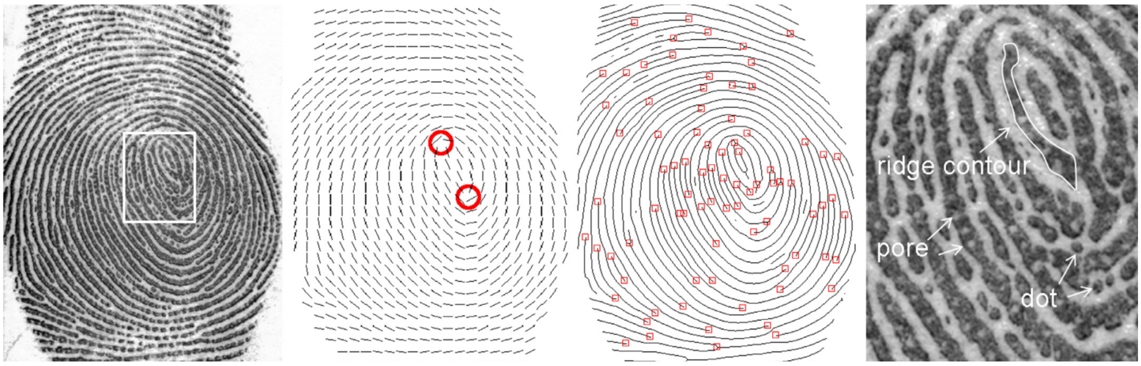


Figure 2.2: Fingerprint features and feature levels

Identifying individuals by their fingerprint is in essence, the comparison between the presented and stored fingerprint template. To enable this comparison, the biometric trait of the individual needs to be known and stored. The first stage of biometric recognition systems, the enrolment stage, enables this. During the enrolment stage, an individual presents his or her fingerprint to the system, enabling the system to acquire the biometric trait and store its template (a mathematical representation). Next, the system extracts a salient feature set and stores this as a template. The next stage of biometric recognition is the recognition stage (depending on the context this might be called verification of identification). During this stage, the individual presents his or her fingerprint to the system which in response will acquire the template, extract the feature set and compares it against the stored template(s). As a result, the system will conclude whether there is a match or an identity which is verified. [49]

Finger vein

Similar to palm vein recognition, the veins or blood vessels in our fingers are sufficiently distinctive to provide verification of an individuals' identity. Like palm vein recognition, this technique uses low intensity infrared light to obtain an image of the blood vessels in our finger. This light gets absorbed by the hemoglobin in blood which will be darker in contrast to the surrounding tissue. [44]

One of the biggest advantages of this technique is its accuracy, since its not susceptible to surface dirt or damage to the physical characteristics of individuals. [90, 38]

Face recognition

The characteristics of our face are something our species has used to recognize one another since the early days of intelligent life itself. In 1964, Woodrow W. Bledsoe and his colleagues initiated the attempt to enable a computer to recognize human faces, with a technology called Automated Face Recognition or AFR. [49]

Since the introduction of AFR, many scholars have attempted to increase the capabilities of such systems. In line with other technological advances, Turk and Pentland popularized Eigenfaces, Penev and Atick used Local Feature Analysis, and in the modern world, Neural Networks (NN) are a key technology enabling the automated recognition of dozens of faces. [49]

Modern face recognition technology has come a long way and is applied in a variety of settings (e.g. Snapchat, unlocking a device, China's surveillance system, and border control systems). Systems currently used at airports use enrollment images stored on e-passports, meaning the images provided by the applicant when he or she is issuing a passport.

Face recognition technologies analyze several features such as the distance between the eyes, the width of the nose, position of cheekbones, the shape and size of the jaw line, the size and shape of the chin, and so forth. [4]

In the last decade face recognition, and in particular 3D face recognition has received a lot of attention. [36] As a result of these advances 3D face recognition technologies and algorithms are now able to process shape and texture together which results in high performance in different poses and illumination conditions. [35] As a result from these development, face recognition has been implemented in consumer products (e.g. Apple's iPhone FaceID). In general, there exists a wide range of 3D acquisition technologies: [35]

- *Stereo acquisition*
  This acquisition technology uses two or more 2D cameras which are calibrated and together create a 3D image of the subject.
- *Structured light methods*
  This technologies combines stereo acquisition with a structured light pattern reflected on the facial surface. The technology also works with a single camera but requires a projection apparatus.
- *Active sensing*
  This category uses a laser beam reflected from the surface and by doing so is capable of measuring distance, creating a range image.

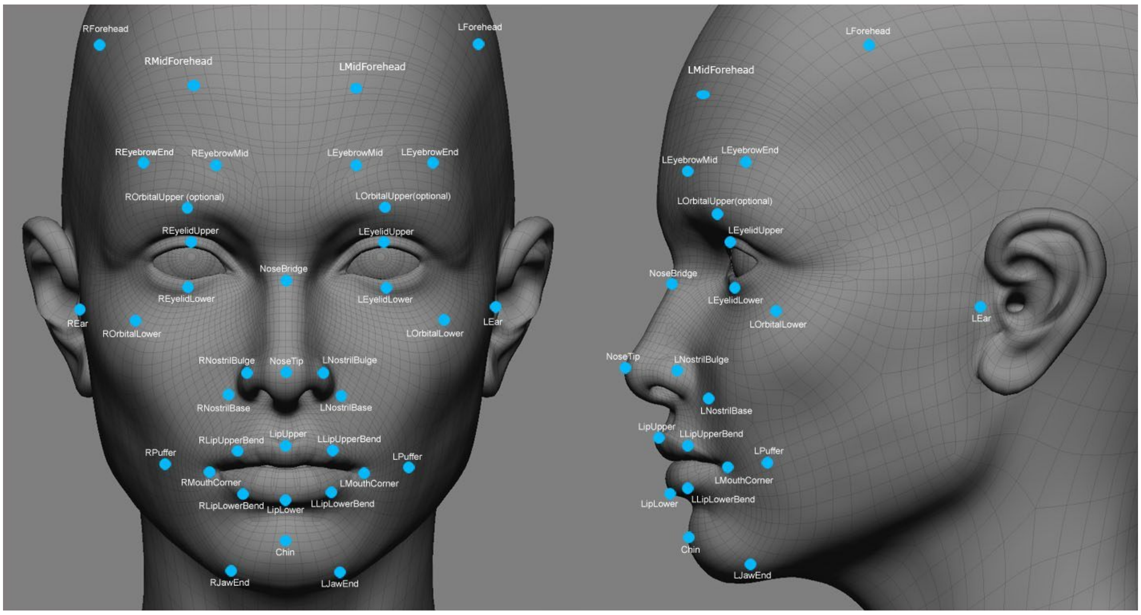


Figure 2.3: Feature extraction of face recognition [99]

Apple's FaceID is an example of 3D face recognition being implemented in consumer products. Apple's technology uses the TrueDepth camera system to create a geometrical map of your face, which is then stored as a mathematical representation in the Secure Enclave Processor (SEP) on the device itself. [3] This technology uses an infrared sensor to create an image of your face together with active sensing. Hence, not only is an infrared image created, but a depth map of your face is also constructed by projecting over 30.000 dots on your face and analyzing them. [3]

Ear

A biometric trait that is lesser-known and characterized by the shape and bone structure are our ears. Some scholars advocate the shape of the outer ear, lobes and the structure of the cartilaginous tissue of the outer area of the ear (pinna area) to be distinctive. Ear recognition technology analyzes the distance of salient points of the outer area of the ear from a so-called "landmark" location on the ear. [83]

Ear recognition is quite similar to the minutiae points of a palm print or fingerprint in the sense that it has many detailed features that can be measured for comparison. [4, 52]

Periocular

Periocular recognition is focused around the area surrounding our eyes, or facial region in the immediate vicinity of the eye. [79] Due to the ease of acquisition of the periocular biometric, it is less invasive to users in contrast to, for example, iris or retina recognition.

Sclera

Beside the iris, scholars argue the potential offered by other parts of the eye for biometric recognition, for example the sclera. Literature dissects the sclera in multiple sub-components ranging from the sclera to the episclera. The sclera, or white area of the eye, can be used to either complement iris recognition, or as a biometric trait on its own. Sclera based identification system use the pattern of blood vessels present in this part of the human eye. [97]

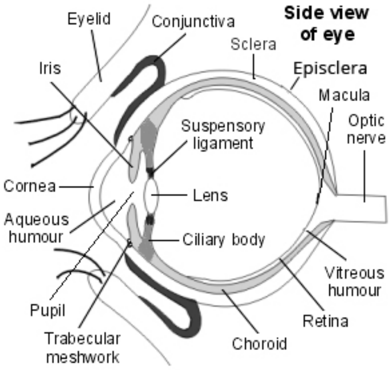


Figure 2.4: Anatomy of the human eye [30]

Iris

As aforementioned, the human eye consists of many components, one of which, the iris (the colored circular membrane surrounding the pupil), is sufficiently distinctive to be used for recognition. [23] Iris based identification systems are increasingly accurate in their matching processes and do so with an increasing speed, indicating a potentially promising future. [52] Based on the arguments from previous research it can be argued that iris recognition might be the most distinctive and trustworthy biometric trait. However, iris recognition systems are usually considered to be intrusive and lack user friendliness. [80]

Electrocardiograph (ECG)

Electrocardiographs (ECG) are proposed by researchers for the identification of individuals in niche market applications. [49] As explained by Irvine et al. an ECG measures the electronic signals emitted by the heart over time using a collection of sensors which are applied to the skin in the chest area. [74, 46]

Scars, marks and tattoos

Scholars often argue the usability of so-called soft biometrics as a supplementing group to hard biometrics modalities (e.g. face, iris, fingerprint). Soft biometric attributes entail an individual's height, gender, ethnicity as well as scars, marks and tattoos (SMT) and are commonly used by law-enforcement agencies for the identification of victims or suspects. [62, 97].

As argued by [62], this type of biometric characteristics provides useful information for the identification of an individual. However, they lack the distinctiveness and permanence to sufficiently differentiate two individuals. Even though SMT lack these properties, they have become increasingly popular for the identification of suspects and victims in forensics and law enforcement situations. [62]

Electroencephalograph (EEG)

An electroencephalograph or EEG is a medical device which uses sensors applied to the scalp to measure electromagnetic signals generated by the brain. This technology is usually used in a medical setting and enables the measurement of information regarding the emotional state, sleepiness or fatigue level, the stress level, as well as continuously measuring the vital signals of an individual. [74]

EEG applied for biometric recognition has several advantages over other biometrics, due to the nature of the signals from the brain, it is extremely confidential and hard to imitate. Furthermore, as research indicates the EEG pattern while under pressure (for example during a robbery) the brainwaves seem to be different and therefor identification through EEG would not be successful at this moment. [57]

Gait

So far we have solely discussed physiological biometrics. However, besides this category academia have also identified behavioral biometrics; characteristics that can be utilized to verify and identity or identify and individual.

The first behavioral biometric trait is human gait. Gait recognition refers to the recognition of an individual based on their distinctive way of walking and overall posture, thus it tries to discover and recognize walking patterns. [74] According to Jain et al. gait recognition is not yet supposed to be very distinctive, but is argued to be sufficiently discriminatory to enable verification in low-security applications. [52] However, a recent article discussed the application of gait recognition in China, although that requires several minutes to operate in order to achieve high accuracy scores. [42]

Keystroke dynamics

A different behavioral biometric characteristic and form of continuous recognition is called keystroke dynamics. Although it can be argued whether this characteristic is unique, it offers sufficient discriminatory information for identity verification purposes. [52]

To do so, a keystroke recognition system analyzes the following distinctive behavioral characteristics: cumulative typing speed, elapsed time between consecutive keystrokes, the time that a key is held down, the frequency of using other keys on the keyboard, and utilized sequence to type capital letters. [23]. Two of the key variables analyzed by keystroke analysis are “dwell time” or “hold time”, which is the amount of time a person holds own one key. The second key variable is “flight time” or “inter-key” or which is the amount they require between hitting keys. [23, 87]

Signature

“*Signature is one of the most accepted methods of asserting someone’s identity. [96]*” This type of behavioral biometric, which is sometimes referred to as dynamic signature analysis, has been widely accepted in government, legal, and commercial transactions as a way of verification. Signature recognition verifies the identity of individuals by analyzing (handwritten) signatures and comparing these with the known signature of that person. [84]

This type of systems not only analyze the shape of a signature, they also rely on the manner in which someone writes a signature. Therefore, it measures: the way in which a signature is written (shape), pressure, pen position, velocity (acceleration) of the pen, length of strokes, tangential acceleration, azimuth and curvature radius. [84, 97, 4]

Voice

A sound of an individuals’ voice is affected by both physiological and behavioral characteristics. Physiological aspects affecting the sound of the voice are: the length of the vocal tract, the general shape of the mouth, size and shape of the lips and nasal cavities. [83] The behavioral characteristics affecting this sound are someone’s speaking habits, for example if an individual grows up in a certain region and therefore acquires an accent characterizing for that area.

To prevent any ambiguity, it is important to clarify the difference between voice recognition and speaker recognition. Voice recognition is merely based on what is being said (which words) whereas the latter is concerned with who says something or speaker verification. [23] Speaker verification is referred to as:“*the automated process of identifying a specific individual’s voice. [83]*” This technology can be applied in two ways: text-dependent or text-independent. Text-dependent recognition is based on the utterance of a predetermined phrase, whereas text-independent recognition is based on solely the voice and independent of what is being said. [52]

2.3 Technology Acceptance theories and models

Information Technology often shows great potential for improving the performance and productivity of employees and business processes in general. However, these potential gains are often obstructed by (future) users or the employees of organizations implementing such systems. Somehow, “supposed-to-be-users” appear to be unwilling to accept and use new systems, often resulting in unsuccessful implementations, a waste of capital and efforts, and a persisting problem. As a consequence, explaining the technology adoption process by users has been a long-standing issue in Management Information Systems (MIS) research which attracted academia and researchers who were interested in the drivers and counteracting factors onctributing to the failure or success of technology adoption. [28] Therefore, we will discuss the collection of TA-research and elucidate on a collection of Technology Acceptance models and corresponding theories established as a result of this attention from acedemia.

2.3.1 Theory of Reasoned Action

Building upon previous theories related to attitude originating from the 1950s/60s, Fishbein and Ajzen developed their *Theory of Reasoned Action* or TRA. In essence, the TRA states that the behavioral intention of an individual is the best predictor of the actual performance of certain behavior. [32, 9] This theory presents a total of five antecedent factors influencing intention and behavior (this model is illustrated in figure 2.5).

As illustrated in figure 2.5, the TRA postulates that the action of performing behavior X can be predicted by an individuals 'Behavioral Intention' (BI) referring to the measure representing the strength of and individual's intention to perform behavior X. According to this theory, the BI is influenced by the subjective norm (SN) and attitude toward the behavior. The subjective norm, which refers to “the person's perception that most people who are important to him think, he should or should not perform the behavior in question [32, p. 302]” is determined by the prior antecedent 'normative beliefs' or the perceived expectations of specific referent groups or individuals, and his or her motivation to comply with the set expectations.

Attitude toward the behavior represents the positive or negative feelings on an individual toward the stimulus. It is noteworthy to mention that this specifically means to the person's own performance of the behavior, instead of its performance in general. [10] This sentiment is determined by the individual's subjective probability that performing a particular behavior will result in a specific outcome. [28, 10, 32, 7]

Since its publication, Ajzen and Fishbein's TRA has been thoroughly analyzed and empirically tested in subsequent research. As a consequence, it has become one of the most widely studied theories relating to user acceptance (Technology Acceptance) theory in MIS research. [19]

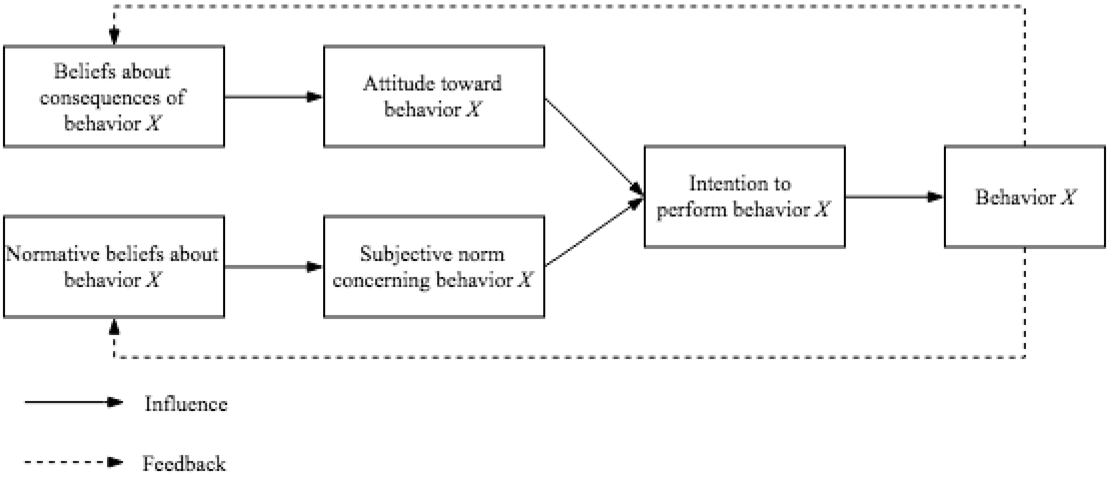

Beliefs about consequences of behavior X
Attitude toward behavior X
Intention to perform behavior X
Behavior X
Normative beliefs about behavior X
Subjective norm concerning behavior X
Influence
Feedback

Figure 2.5: Theory of Reasoned Action [32, p. 16]

2.3.2 Theory of Planned Behavior

Where the TRA focuses on the psychological determinants of behavioral intentions and human behavior in respect to volitional behavior, Ajzen's Theory of Planned Behavior (TPB) was developed as an extension focusing on non-volitional behavior. [9] As aforementioned, the TPB is considered as an extension of the TRA and is based on the rationale that, usually, humans behave sensibly and take account of available information and implicitly or explicitly consider the implications of their actions. [7] In addition to the TRA, the TPB incorporates the factor 'Perceived Behavioral Control' (PBC) (illustrated in figure 2.6). This factor illustrates the degree to which an individual has control over both the internal, and external factors that might interfere with the execution of intended behavior, thus emphasizing the difference between volitional and non-volitional behavior.

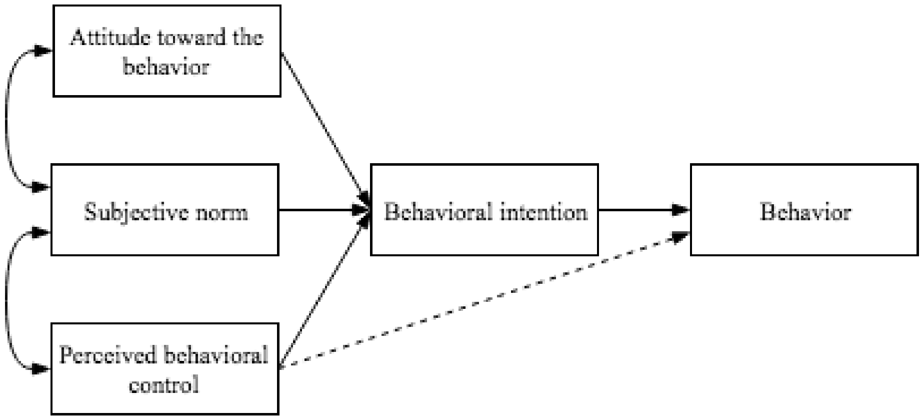


Figure 2.6: Theory of Planned Behavior [7]

In essence, the TPB concludes that if an attitude and subjective norm regarding a specific behavior are more favorable, and the greater perceived behavioral control is, an individual's intention to perform the behavior should be stronger.

2.3.3 Technology Acceptance Model

As discussed in previous paragraphs, an important and lasting issue with MIS and IT in general is the resistance originating from future users. Due to the tremendous investments in IT project, this resistance combined with the risk regarding the return on investments (ROI), has been part of Davis' motivation to attempt improving the ability to predict, explain, and increase Technology Acceptance and innovation adoption. Resulting from his dissertation titled: 'A Technology Acceptance Model for empirically testing new end-user information systems: theory and results' [26] and further research, the so-called Technology Acceptance Model (TAM) has been developed (illustrated in figure 2.7). [28]

Davis' TAM is considered to be an adoption of Ajzen's and Fishbein's TRA [10, 32] with the specific goal of modeling the user acceptance of information systems (IS). Davis' model attempts to achieve this by focusing on six individual components and relations connecting them (see figure 2.7 for the illustration). Building on the foundation laid by Ajzen and Fishbein, the TAM adds two factors which Davis deemed of primary relevance for computer acceptance behaviors: Perceived Usefulness and Perceived Ease of Use, while excluding 'subjective norm'. Perceived Usefulness refers to: "The prospective user's subjective probability that using a specific application system will increase his or her job performance within an organizational context." [28, p. 985] Perceived Ease of Use refers to: "The degree to which a prospective user expects the target system to be free of effort."[28, p. 985] As mentioned by Davis and acknowledged by Fishbein et al, subjective norm (SN) is one of the least understood components of the TRA. [28] Due to this lack of understanding, it was decided to exclude this factor from the TAM.

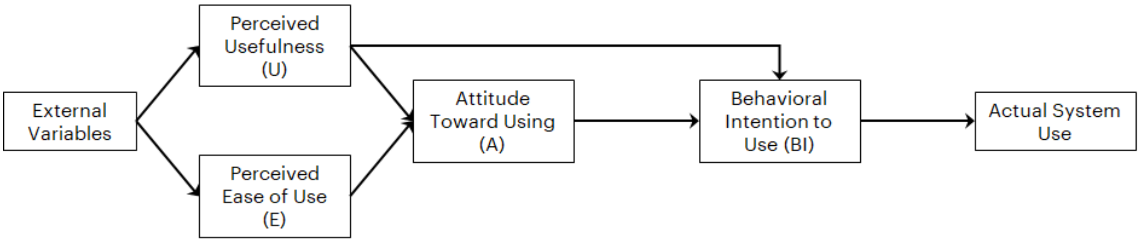

Perceived Usefulness (U)
External Variables
Perceived Ease of Use (E)
Attitude Toward Using (A)
Behavioral Intention to Use (BI)
Actual System Use

Figure 2.7: Technology Acceptance Model [28, p. 985]

In summary it can be concluded that while the TRA postulates that BI is determined by the attitude and subjective norm (BI = A + SN), the TAM postulates that behavioral intention is determined by both the attitude and perceived usefulness (BI = A + U).

2.3.4 Innovation Diffusion Theory

Rogers' Diffusion of Innovation theory (DOI or sometimes referred to as IDT) originates from the 1960s and is considered as one of the primary theoretical frameworks for understanding and explaining individuals adoption behavior of new technologies. [81, 85] Although the theory finds its roots in the field of sociology, it is used in a wide range of disciplines ranging from political science to communications economics, and especially IS. [54]

Rogers' theory advocates that an individuals' willingness to adopt an innovation varies based on their 'innovativeness'. Based on this line of reasoning he has defined five categories of adopters: innovators, early adopters, early majority, late majority, and laggards. [85] The DOI model suggests that the decision to adopt or reject an innovation by the individual, is predicated upon five key perceptions:

- *Relative advantage*
  Which is defined by Moore and Benbasat as:"*The degree to which using an innovation is perceived as being better than using its precursor. [73, p. 195]*"
- *Compatibility*
  Which, according to Pham et al. refers to:"*... how well a technology fits an individual's working style, lifestyle, values and needs. [5, 85, 81]*" To prevent ambiguity, it is worth mentioning that this construct is not related to the compatibility of either software or hardware components but rather to technology as a whole in relation to the lifestyle of an individual.
- *Complexity*
  This construct is often argued to be similar to Davis' 'Perceived Ease of Use' construct. According to Moore and Laukkanen et al. it refers to: "*... the degree to which an individual considers an innovation to be relatively difficult to understand and use.*" [73, 61]
- *Observability*
  For an innovation to find its way to our everyday lives, it needs to be observed and experienced by (potential) adopters. Therefore, Rogers' theory incorporates the observability of an innovation and defined it as: "*... the degree to which the results of an innovation are observable to others. [21, p. 620]*"
- *Trialability*
  If a person gets the opportunity to become more experienced and comfortable with a certain innovation, it is suggested that this person becomes more willing to adopt. Thus, Trialability is defined as: "*the degree to which an innovation might be experimented with on a limited basis. [73, p. 195]*"

2.3.5 Unified Theory of Acceptance and Use of Technology

A different and more comprehensive attempt to understand, explain, and better predict Technology Acceptance, is Venkatesh et al.'s Unififed Theory of the Acceptance and Use of Technology or UTAUT. This team of researchers aimed to combine exisiting TA models' constructs into one, all-encompasing theory, resulting in one TA model and thus getting rid of any ambiguity associated with previous models and theories. [102]

Resulting from their extensive study of existing TA models, Venkatesh et. al developed their UTAUT model as presented in figure 2.8. To begin with the factor 'Performance Expectancy', Venkatesh et al. have defined this factor as: *"the degree to which an individual believes that using the system will help him or her to attain*

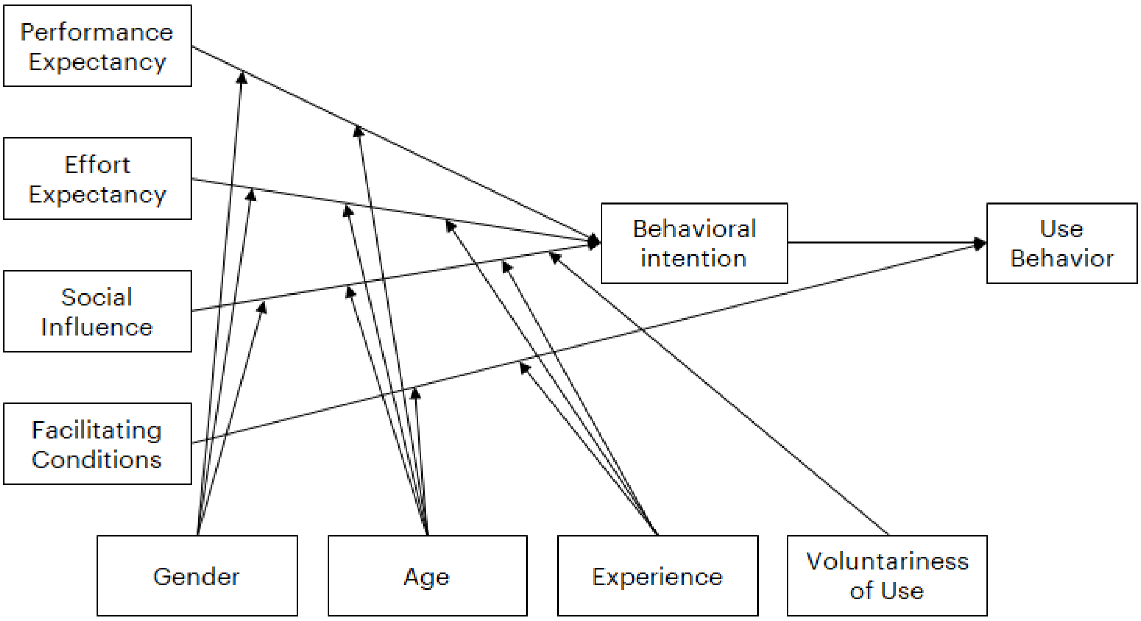


Figure 2.8: Unified Theory of Acceptance and Use of Technology [102, p. 447]

gains in job performance. [102, p. 447]". The second factor 'Effort Expectancy' has been defined as: *"The degree of ease associated with the use of the system. [102, p. 450]"* The third factor 'Social Influence' has been defined by Venktesh et al. as: *"The degree to which an individual perceives that important others believe he or she should use the new system. [102, p. 451]"* Finally, the last factor 'Facilitating Conditions' was defined as: *"The degree to which an individual believes that an organizational and technical infrastructure exists to support the use of the system. [102, p. 453]"*

Unified Theory of Acceptance and Use of Technology 2

As aforementioned a variety of models have been developed from which Venkatesh's UTAUT has just been described. This model has been applied by many scholars to study the technology acceptance of a wide range of technologies. As a result, its validity has been thoroughly tested. These studies, however, often applied a sample of the factors originating from the UTAUT, enabling these studies to focus on other hypothesized factors influencing technology adoption.

In reaction to this trend, Venkatesh et al. have developed a new model, the UTAUT2 [101]. UTAUT2 is an extension of UTAUT that explicitly aims to study the Technology Acceptance in a consumer context. In addition to the UTAUT, UTAUT2 includes three additional constructs: hedonic motivation, price value, and habit.

In their paper, Venkatesh et al. state that hedonic motivation is a factor which contributes to the consumer's intention to use technology, a statement that is based on previous research (e.g. [98, 95]. It has been defined as: *"the fun or pleasure derived from using technology. [101, p.161]"* Furthermore, Venkatesh et al. suggest that the price of technology is an important factor in the context of consumer use.

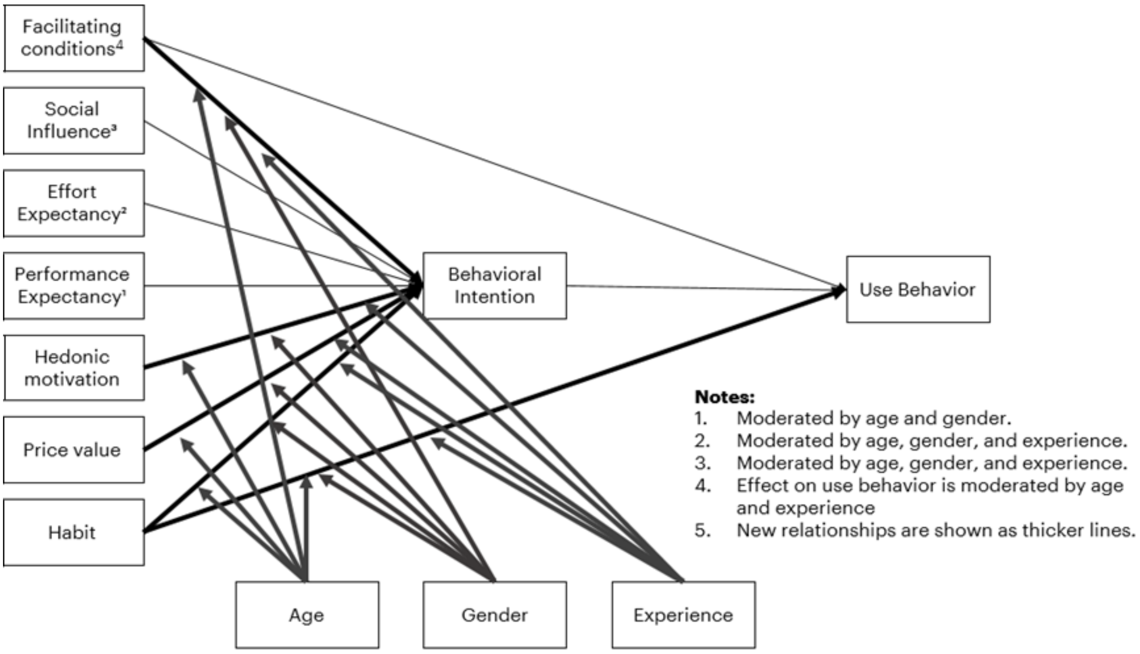

Facilitating conditions4
Social Influence3
Effort Expectancy2
Performance Expectancy1
Hedonic motivation
Price value
Habit
Behavioral Intention
Use Behavior
Age
Gender
Experience
Notes:
1. Moderated by age and gender.
2. Moderated by age, gender, and experience.
3. Moderated by age, gender, and experience.
4. Effect on use behavior is moderated by age and experience
5. New relationships are shown as thicker lines.

Figure 2.9: Unified Theory of Acceptance and Use of Technology 2 [101]

Where in the organizational context the end-user does not have to pay for a certain technology, the individual consumer does. Thus, price value is defined as *"consumers' cognitive trade-off between the perceived benefits of the application and the monetary cost for using them. [101, p. 161]"* Lastly, habit is defined as *"The extent to which people tend to perform behaviors automatically because of learning, equate habit with automaticity. [101, p. 161]"*
Besides the addition of three new constructs, the UTAUT2 model also incorporates several new relations (presented as bold lines in figure 2.9.

2.4 Conceptual model

This study aims to develop, and empirically test, a conceptual Technology Acceptance model regarding the acceptance of biometric authentication on mobile devices for the authorization of financial transactions. We develop this model by drawing on the extant literature on human decision making, technology acceptance and innovation adoption (see previous paragraphs). In this study variables originating from a variety of other models were adapted: from Davis' TAM we included the variable 'Perceived Ease of Use' (PEoU), and from Rogers' DOI (or IDT) we included the variables 'Compatibility' (which we renamed to Lifestyle Compatibility and abbreviated to LC) and 'Innovativeness'. Drawing from security, privacy and risk literature, we included the variables 'Perceived Privacy' (PS), 'Perceived Risk' (PR), and 'Perceived Security' (PS). Each of these constructs are implemented in our model with the final goal of determining the Behavioral Intention (BI) of consumers.

In our case we aim to investigate how these variables differ between the technologies and transaction values presented in the scenarios.

2.4.1 Variables and hypotheses

Lifestyle compatibility

John Gourville, famous for his Harvard Business Review article “Eager Sellers and Stony Buyers” [37], designed a behavioral framework in which he proposes the characteristics of so-called ’easy sells’ and ’smash hits’. According to his research, an innovation requiring little behavioral change(s) will be an easy sell and has the potential to become a smash hit. Following his line of theory, it can be hypothesized that if someone’s habit is to unlock their mobile device using a biometric modality (e.g. fingerprint or face), using the same method to authenticate payments requires no behavioral change. Hence, there will be little to no resistance from the behavioral change perspective. This line of thought has been incorporated in a wide variety of TA-related research and can be linked to the construct ’Compatibility’ originating from the IDT. [85] In their research regarding the TA of NFC-based mobile payments, Pham et al. developed a conceptual model which included the construct ’Compatibility’ as a product-related factor predicting Behavioral Intention. [81]

Resulting from their analysis, the hypothesis that Compatibility would have a positive effect on the Behavioral Intention to adopt NFC mobile payments has been supported. Thus, individuals who consider a technology to be compatible are more inclined to technology adoption or adoption of an innovation. This association between Compatibility and Behavioral Intention was confirmed to the degree in which Compatibility was considered one of the key determinants for the spread (adoption) process of innovations. [81]

Research by [72] shows that Compatibility was one of the most significant factors positively contributing to the Behavioral Intention of accepting iris scanning for the facilitation of person-bound services. Other research showed the importance and significance of Compatibility in the context of mPayments in general [77, 22], mBanking [106], and the adoption of mBanking over time, showing the importance of Compatibility for both current and potential users/adopters. [108]

To prevent ambiguity, we maintain the term ’Lifestyle Compatibility’ (LC) to address the construct referring to: *... how well a technology fits an individual’s working style, lifestyle, values and needs. [5, 85]* With the incorporation of this construct in our model, we want test a notion by Saaksjarvi, saying: consumers who feel that the new product or service is not in tact with their past experiences, values and needs are likely to reject the product or service before it enters their consideration sets. [86] Thus, we propose the following hypotheses:

Hypothesis 1a: The greater the Lifestyle Compatibility, the greater the Behavioral Intention.

According to Rogers’ Diffusion of Innovation theory, the willingness of individuals to adopt innovations varies based on their degree of innovativeness. In his study five categories of innovativeness are identified: those who want to experiment with the technology when it first launches called innovators (or the 2.5% of the population), early adopters (13.5%), early majority (34%)), late majority (34%)), and laggards (16%)). [85] Based on this scale we have a spectrum with on the one end innovators who are willing to be the first to try a new technology. [54, p. 114]. While on the other side, there is the group of individuals who will only adapt if they have to. Therefore, we propose the following hypothesis:

Hypothesis 1b: The influence of Lifestyle Compatibility on Behavioral Intention to accept biometric authentication will be moderated by innovativeness, so that the effect will be stronger for highly innovative individuals.

Perceived Ease of Use

Perceived Ease of Use (PEoU) which has been defined as: *"The degree to which a prospective user expects the target system to be free of effort [26, p. 985]"* has been identified as an important factor in TA-research. Miltgen et. al have discovered an association between Lifestyle Compatibility and Perceived Ease of Use regarding the use of iris recognition to facilitate person-bound services. [72] These findings are further supported by Koenig-Lewis et. al, who proved the significance of this association in the case of mBanking adoption. [59]

Since this study is interested in the mobile authentication of payments using different recognition technologies, it is closely related to research focusing on mBanking, mPayments and eBanking on mobile devices. Therefore, we strongly believe that the same association will be discovered in our study, hence we propose the following hypotheses:

Hypothesis 2a: The greater the perceived Lifestyle Compatibility, the greater the Perceived Ease of Use.
Hypothesis 2b: The influence of Lifestyle Compatibility on Perceived Ease of Use will be moderated by innovativeness, so that the effect will be stronger for highly innovative individuals.

The Behavioral Intention to accept a certain technology or innovation has long been the final variable in which researchers are interested. Since the introduction of the Theory of Reasoned Action (TRA) it has been defined by Ajzen and Fishbein as: *"an individual's subjective probability that he or she will perform a specified behavior." [32, p. 288]"*
According to Davis' research, the attitude toward using a technology (either positive or negative) leads to the behavioral response of using a system. This attitude is determined by two cognitive responses, one of which is the Perceived Ease of use. The TAM theory postulates the importance of design features' direct influence on the PEoU and the influence of PEoU on the Behavioral Intention. [26] "*...Perceived Ease of Use has been repeatedly identified as an important issue governing user acceptance processes. [26, p. 34]*"

The findings regarding the predicting capability of PEoU to BI contradict each other so that here is no clear consencus. In prior research regarding the acceptance of iris recognition, Miltgen et. al discovered that a greater PEoU did not result in a greater BI. [72, p. 109] Oliveira et. al discovered that Effort Expactancy, the UTAUT variable similar to PEoU, did not significantly predict the Behavioral Intention to adopt mPayments. [77] However, research by Huys shows that in the case of iris recognition combined with face recognition, and fingerprint recognition separately, this hypotheses was confirmed for a physical retail store. [43]

Thus, we propose the following hypothesis:

Hypothesis 3: The greater the Perceived Ease of Use, the greater the Behavioral Intention.

Perceived Risk

According to research by Lu et al. approximately 75% of consumers are worried about security and transaction risk. [68] Behavior of consumers can generally be considered as an instance of either taking or reducing risk. [94] Therefore, research proposes (perceived) risk as an important factor influencing human decision making, buying decisions, and technology adoption in particular. Wessels and Drennan have defined Perceived Risk (PR) as: *"the consumer's belief regarding the likelihood of suffering a loss in pursuit of a goal. [106, p. 551]"* The occurrence of this 'loss' can either occur in case of the purchase of a product or a service, however, there appears to be a difference between the risk perception of products and services. A body of knowledge has found a consensus regarding the higher levels of uncertainty related to services, causing them to be considered as more risky in comparison to products. [81]

The higher levels of uncertainty, and consequently Perceived Risk related to services, pose a potential barrier to technology adoption by consumers. [60] Since financial transactions are a service provided, or supported, by payment service providers (PSPs) and banks, we strongly believe that risk will either be an important driver of or inhibitor to technology acceptance.

The influence of PR on BI has been studied in a variety of settings, focusing on different innovations: Kesharwani et. al studied the affect of PR on BI in case of the adoption of Internet banking (or eBanking). [56] Pham et. al found PR to be the fourth most importance factor affecting intention to adopt NFC mobile payments (mPayments). [81] Miltgen et. al proved that PR has a direct effect on BI regarding the usage of iris recognition for person-bound-services. [72] Curran et. al, discovered PR to have a significant negative effect on intention to use mBanking. [24] Overall, this research concluded that the higher a consumers' belief regarding the likelihood of suffering a loss, the lower the probability that they will intend to use the innovation or technology. Therefore, we propose the following hypotheses:

Hypothesis 4a: The greater the perceived Lifestyle Compatibility, the smaller Perceived Risk.
Hypothesis 4b: The influence of Lifestyle Compatibility on Perceived Risk will be moderated by innovativeness, so that the effect will be stronger for highly innovative people.
Hypothesis 5: The greater the Perceived Risk, the lower the Behavioral Intention.

Perceived Privacy Concerns

A report from 'Maatschappelijk Overleg Betalingsverkeer' states that the privacy of customers is of utmost importance. It discusses the privacy risk related to the usage of biometric authentication and mentions that the biggest risk associated with biometrics is the leaking and improper use of the stored characteristics (or templates). [17]

Given the personal nature of biometric technologies, their adoption may be inhibited by individual's concern for information privacy. [31] A concern for many consumers is the irrevocability of biometric characteristics. In case of a data breach, nowadays one can easily change their user name of password. When using biometrics, however, this is not longer possible since *you* are the password. Therefore, one of the biggest issues related to the widespread acceptance of biometric authentication is the fear of hackers obtaining the biometric data provided by consumers. [17]

Privacy concerns are an important factor in successful biometric implementation and adoption by consumers. [89] Despite the attention given to privacy and security concerns, Miltgen et. al found that: *"Although the issue of privacy has emerged as a major inhibitor of biometrics acceptance, the research on this issue is quite rare to date, especially from the viewpoint of customers. [72, p. 104]"* Thus, we want to discover what influence the Perceived Privacy Concerns will have in our scenarios and propose the following hypotheses:

Hypothesis 6a: The greater the perceived Lifestyle Compatibility, the smaller the Perceived Privacy Concerns.
Hypothesis 6b: The influence of Lifestyle Compatibility on Perceived Privacy Concerns will be moderated by innovativeness, so that the effect will be stronger for highly innovative people.
Hypothesis 7: The greater the Perceived Privacy Concerns, the smaller the Behavioral Intention.

Perceived Security

Issues or concerns regarding the security of biometric authentication can form a barrier for customers to adopt a certain technology. [22, 53] Therefore, it can be concluded that security is an important aspect of electronic devices and especially for electronic payment systems. Tassabehij et. al have studied the effect of 'Perception of Biometric-Banking Security' on the 'Intention to Use' regarding biometric authentication for eBanking and concluded that there was a direct positive association. Hence, in this specific research, perceptions of b-banking security was found to be one of the key determinants leading to usage of the system. [93]

In our study we defined Perceived Security as the degree to which a user of the recognition technology feels protected against security threats related to using such a technology for user authentication to authorize financial transactions. [76] A greater perception of the security of a technology, product, or service, will most likely result in a more positive intention to adopt. Based on this line of reasoning, we draw the following hypotheses:

Hypothesis 8a: The greater the perceived Lifestyle Compatibility, the greater the Perceived Security.
Hypothesis 8b: The influence of Lifestyle Compatibility on Perceived Security will be moderated by innovativeness, so that the effect will be stronger for highly innovative people.
Hypothesis 9: The greater the Perceived Security, the greater the Behavioral Intention.

2.4.2 Demographics

Research by Shaikh and Karjaluoto has indicated the importance of age, gender and education level of respondents regarding the adoption of M-banking [92]. Venkateh et. al included age and gender in the development of their UTAUT models as well and found these factors to have a moderating effect on some associations [102]. Demographic details (e.g. age, gender, and education level) have therefore been included in our model due to the potential impact they might have on the adoption of various technologies.

2.4.3 Control variables

For our study, a total of three control variables have been identified. The first variable that could have any effect on the results of the research is the experience respondents might have with the biometric technology. Venkatesh et al. elaborate on the effect prior experience can have on an individual's attitude towards a technology and their intention to adopt it. [102] Fishbein and Ajzen, state that positive or negative experiences with a product or service in the past will have a decisive impact on future behavior (behavioral intention). [32] Hence, researchers have included it as a moderator in their research frameworks ([34, 58, 65]) which indicated the significant effect experience has on behavioral intention.
The second variable that could influence the results of the research is the price incorporated in the scenarios presented to respondents. Although the aim of this research is to discover the Technology Acceptance of biometric modalities (e.g. fingerprint recognition and facial recognition as well as pattern recognition) in the case of payment authentication, the price of a purchase is of lower relevance. The main reason for incorporating a price is to discover potential differences in preferences between the technologies in relation to the amount of a purchase, and the constructs. As discussed by the permitted transactions, in our case for example per technology, could depend on the amount of a transaction and/or the transfer to recognized account numbers. This is already implemented in the current Dutch wireless payment system: purchase amounts up to 25 euros can be paid wireless without any PIN, values above this threshold require the customer to provide their PIN. The reason behind this, is the risk associated with these payments (it is often described as Risk-Based Transactional Authentication Payment values.
Finally, another variable that might influence the results of the research is the (biometric) recognition technology presented to the respondents, in our case either

fingerprint recognition, facial recognition or pattern recognition.

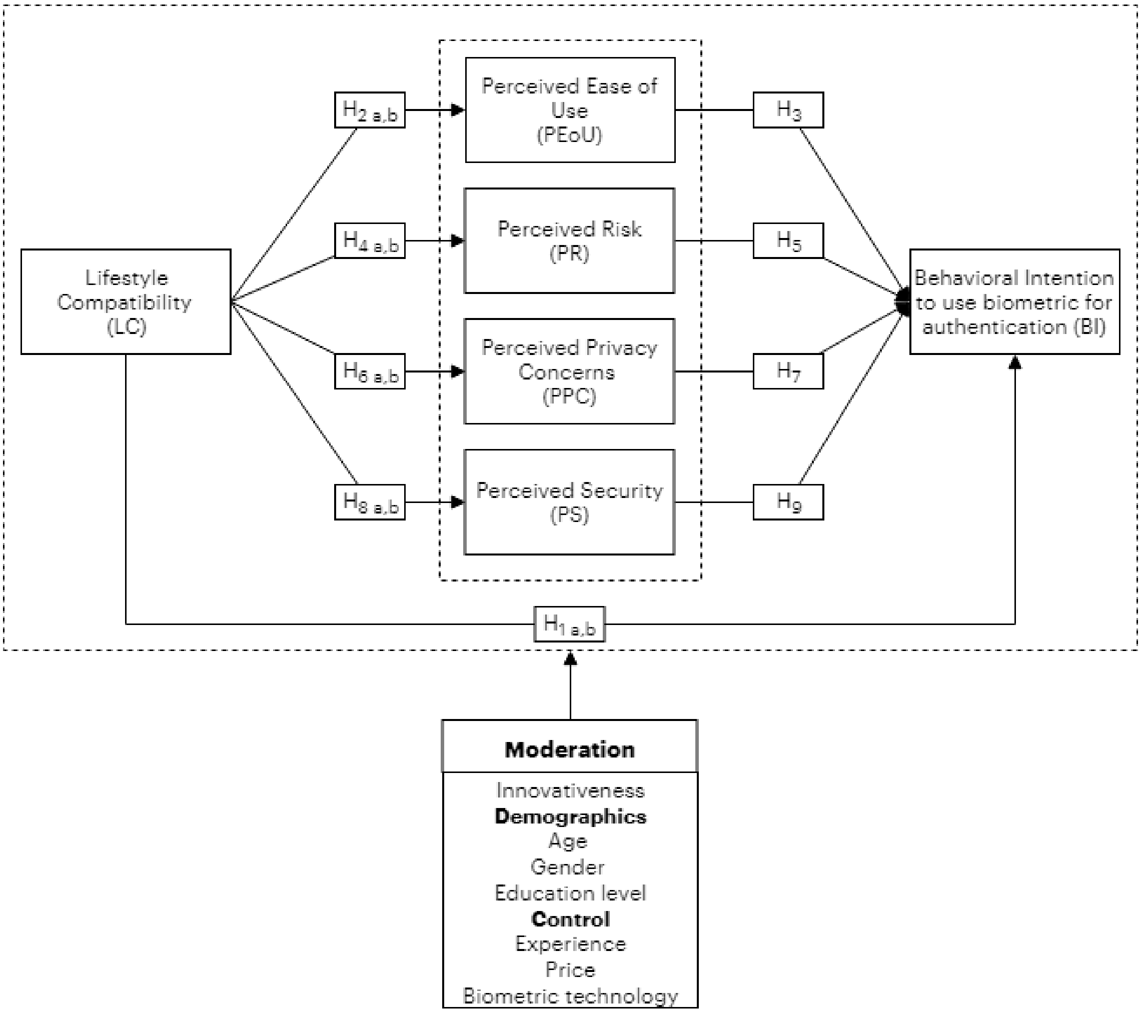


Figure 2.10: Research Framework applied in this study

Chapter 3

Methodology

3.1 Biometric technology selection

At the beginning of the prior chapter, we discussed the wide variety of existing biometric modalities. After illustrating the variety of modalities in a tree diagram, we provided a brief description of every biometric modality. As one can conclude from this overview, the possibilities of biometric modalities are plentiful. However, due to the focus of this research, the acceptance of biometric authentication methods on mobile devices, we are limited in the number of modalities that can be applied.

First of all, the current technological capabilities of smartphones and tablets, made us decide that modalities that require big, or extremely high-tech medical machines are not suitable options for our research. Hence, DNA (which requires thorough analysis of for example, blood), Electrocardiograph (ECG, which requires a heart-beat sensor), Electroencephalograph (EEG, which requires some kind of hat that measures brain waves), Palm vein (which requires infrared light and sensors), and finger vein (which requires infrared light and sensors) were excluded.

Other biometric modalities such as hand geometry also require devices that are to large to be incorporated in mobile devices. The current technologies used for the recognition of the hand geometry, as well as palm print, are at least the same size as the hand itself. Therefore, this modality is not suitable for applications in a mobile setting. [1, 23, 52]

Due to the impact incorrect authentication could have on the financial situation of consumers, the criteria “distinctiveness” is one of the top priorities. Due to the lack in distinctiveness and permanence, the attributes of the so-called “soft-biometrics” such as scars, marks and tattoos (SMTs) are not suitable for this application. [97, 62]

Ear recognition, which is advocated by some biometricians, is not a suitable modality due to its low ease of use. If one would like to use this type of technology on a mobile device it would be required to take a picture of your ear, which could be covered with hair or a hat. [84] Furthermore, the degree of distinctiveness is also argued by multiple scholars. [52]

Gait recognition, e.g. the recognition of an individual based on the way he or she walks as measured by the accelerometers and gyros in the mobile device. This biometric modality is hard to trace using a tablet. Especially since this will most likely measure the rhythm of steps instead of step length as possible by a smartphone located in one's pocket. This technology is especially useful for surveillance purposes and less so for verification of an individual's identity to authenticate financial transactions. Due to the relative low level of accuracy, it is not the best modality to use due to the low level of distinctiveness and permanence. [92, 52]

The most well-known technologies currently in use for the recognition of individuals are limited to just five: fingerprint, facial, iris, hand geometry, and voice recognition. [72] As aforementioned, hand geometry is not a suitably modality to be used on mobile devices. From the remaining technologies, we can see in figure 3.1 that the distinctiveness, permanence, and performance of keystroke, signature, and voice recognition are low. Hence, we exclude them from our study.

Parusheva compared biometric technologies for the authentication of consumers in eBanking and concluded that fingerprint recognition, iris recognition, and facial recognition are the three most suitable technologies for this specific use case. This conclusion is based on his analysis of five other papers comparing a total of seven biometric modalities. The three aforementioned biometrics received scores of 16.2, 16.0 and 15.2 respectively. [80] Throughout the years, other researchers also compared the various biometrics with changing conclusions throughout the years. Based on articles from Parusheva and Jain et. al, we see the improvement of facial recognition as a biometric modality. [52, 80]

Since our study is focused on the technology acceptance of consumers, iris recognition is not presented as one of our scenarios. According to Jain et. al this biometric modality has the lowest acceptability (see table 3.1). This argument, in combination with the time and resource constraints of this study, led us to the decision to include the two remaining biometric technologies: fingerprint recognition and facial recognition. We will elaborate on these scenarios in a later paragraph.

	Factors						
Biometric identifier	*Universality*	*Distinctiveness*	*Permanence*	*Collectable*	*Performance*	*Acceptability*	*Circumvention*
Face	H	H	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Hand geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Table 3.1: Comparison of different biometric modalities [51]

As the paragraphs above describe, a wide range of biometric modalities have been identified. From this collection, several are more suitable for implementation on mobile devices. These technologies might be considered as competition to the old-fashioned and well-known Personal Identification Number (PIN) or passwords. However, since the introduction of smartphones, a different kind of security mechanism has been introduced: pattern lock.

Pattern lock, which relies on pattern recognition, is a graphical approach that might be familiar to smartphone users, and especially Android users. The rationale behind the development of graphical authentication methods is that humans are better in remembering pictures than text. [39] A prominent example of a graphical approach ensuring secured access to mobile devices, has been developed by Google with the name 'pattern lock' (a drawmetric system). Pattern lock technology uses 9-points (a 3x3 matrix) which a user can connect in order to create his or her pattern. By connecting the dots of the pattern, the technology checks if the pattern is correct and if so, provides or restricts access to the device and the information stored on it. [104]

Research by Malkin et al. indicate that roughly a third of all users who have a smartphone, unlock their device using pattern recognition. While from all users who lock their smartphones, 48% use pattern recognition as a locking mechanism. [69] Although, theoretically, a 3x3 matrix offers 389.112 distinct patterns for 9-point combinations, users' bias in pattern choice result in using only a small fraction of these possibilities. [104]

Despite the high number of users, the technology itself is not considered as safe or secure. Some security vulnerabilities of such systems are: shoulder surfing, which entails an attacker looking (physically) at the device when the user enters his or her pattern, social engineering, where the attacker somehow tricks the user to describe the pattern, and phishing attacks. Although shoulder surfing is a cause for concern in case of passwords as well, pattern lock has the additional disadvantage of smudge attacks. [18, 12] This type of attacks entail that an attacker has physical access to the device and is able to discover the pattern by looking at the traces of grease left on the screen.

Due to this widespread adoption of pattern lock, and its associated security issues, we decided to incorporate it in this study as a comparative technology that could serve as a distraction.

3.2 Questionnaire design

3.2.1 Purpose and type of questionnaire

> "*Questionnaires are often part of a survey strategy to collect descriptive and explanatory data about facts/demographics, attitudes/opinions and behaviours/events. [70, p. 481]*"

According to Saunders et al, a questionnaire is the most widely used method to collect data within the survey strategy. Our study used a cross-sectional questionnaire to discover the Technology Acceptance of consumers regarding biometric authentication methods on mobile devices for the authorizations of financial transactions. Hence, the data will be collected at one point in time (i.e. a snapshot). [70]

The questionnaire was designed using the online tool 'Qualtrics' for which a license was obtained via Leiden University. Based on the typology of Saunders et al, it can be characterized as a self-completed web and mobile questionnaire that was distributed via Qualtrics' built-in options (e.g. Facebook, LinkedIn and mail) as well as via direct text messages. [70] The service provided by Qualtrics ensured the accessibility of the questionnaire and enabled respondents to access it using either their computers' internet browser or mobile phone. Besides providing a URL to navigate to the survey, Qualtrics also provided the option to present a QR-code which, when scanned by a regular smartphone, directly links the respondent to the correct page. Hence, this functionality increased the accessibility of our survey and the ease with which individuals could participate in this study. When the data collection was completed, we exported this by using Qualtrics' export functionality which offered the option of exporting it to a format compatible with IBM's statistical software 'SPSS 25'.

3.2.2 Scales and Items

The questionnaire used in this study was developed using previous TA-research as a foundation and consisted of five sections. These sections are: the introduction, demographic details and innovativeness, the scenario (one per respondent), questions corresponding to the constructs from the conceptual model, and finally an option to leave remarks and contact details.

The overall structure of the survey, for which the items can be found in Appendix B, is as follows:
First of all, every respondent was introduced to the questionnaire using the introduction. As advocated by Saunders et al. the introduction was used to explain clearly and concisely why we would like the respondents to answer our questionnaire. [70] Second, questions regarding the demographics characteristics of the respondents were presented. We asked them for their gender (male, female, or other), their age, and highest obtained educational degree (based on the Dutch educational system). For an overview of the demographic information of our respondents see table 3.2. Third, several questions regarding 'Innovativeness' were presented to the respondents. To measure an individual's innovativeness, we applied four questions often used by other TA-related research (e.g. [94, 108, 107]) originating from Agarwal et. al. [6] These four questions use a seven-point Likert scale varying from 'totally disagree' to 'totally agree'. We incorporated innovativeness as a variable due to the expected moderating influence on relations in our conceptual model. [66] Fourth, every respondent was presented with one of the six scenarios (illustrated in figure 3.1 and included in Appendix A. These scenarios are the key component of our study since they provided the context of the situation in which the biometric authentication is applied. Fifth, the control variable 'Experience' is answered using two questions asking respondents for their experience using the recognition technology presented in the scenario and the mobile banking app. This variable is incorporated because of the affect it could have on the constructs. Although Lifestyle Compatibility and experience might sound the same. The difference lies in the fact that the experience is related to the specific technology and Lifestyle Compatibility is focused

on the method being compatible with one's lifestyle. Consequently, the questions regarding the constructs incorporated in our conceptual model are presented to the respondents. For the constructs Lifestyle Compatibility (LC), Perceived Ease of Use (PEoU), Perceived Risk (PR), Perceived Privacy Concerns (PPC), Perceived Security (PS), and Behavioral Intention (BI), questions were adapted from [22, 27, 81, 22, 93, 102] respectively. The development of the survey will be discussed in the following paragraphs.

3.2.3 Development and validation

The design and validation of the survey used for this study was based upon the iterative process of the Design Cycle, key component of Design Science Research. [40] This methodology applies an iterative cycle consisting of steps of building or refining the artifact and then evaluating it. As mentioned by Hevner (2007):"*artifacts must be rigorously and thoroughly tested in laboratory and experimental situations before releasing the artifact. [40, p. 5]* " We applied this process to design our survey, resulting in the following iterations:

First iteration

After establishing the conceptual model, the first step in the development of the questionnaire consisted of gathering the questions related to each construct (questions were adapted from prior research: [22, 27, 81, 22, 93, 102]). The questions related to every single construct originate from a single source. By doing so, we are able to guarantee the validity and prevent any issues that might occur as a consequence of combining multiple studies to address a single construct. Together with the introduction and scenarios, this version of the survey was sent to experts and some minor changes to formulation were implemented. This adjusted version was then presented and tested rigorously by participants of the pilot test (N = 15; 9 males, 6 females). Due to potential score differences related to age of respondents, the participants originate from different age categories: 18 till 24 (N = 9), 25 till 34 (N = 4), and 55 till 65 (N = 2).

To ensure consistency and prevent uncontrolled effects, the same structure throughout every individual session with participants was maintained. First, the procedure for the session was explained to the participant after which they were handed the iPad which would be used to complete the survey. The instructions presented to participants were: complete the survey as if you are at home, give a sign when you are done with the statements presented on the current page before continuing, mention everything that comes to your mind while completing the survey. During the completion of the survey, participants' reactions were observed and if a reaction was noticed, they were asked to elaborate on their thoughts, resulting in a thorough understanding of participants' emotions, perceptions, and potential errors in the questionnaire.

Following the structure of the survey, we asked participants to read the introduction and briefly state their interpretation of the topic, goal, and purpose of both the survey and study in general. By asking this question, we were able to conclude whether the introduction provided a clear and precise description of the study. Feedback from the participants was recorded in a separate document, specified by the corresponding part of the survey (and the specific question).

As a result of these sessions an extensive document with feedback was obtained, as well as a first indication of what the data would look like. Based on the feedback obtained from this pilot group we implemented several changes. However, for a change to be implemented it had to meet one key criterion, namely whether this specific remark was stated by more than one participant. The line of reasoning behind this is that is multiple respondents thought something was unclear, this would be triangulated and hence must be correct. Based on these sessions we implemented multiple changes: questions regarding innovativeness were clarified by specifying what "information technologies" are. Furthermore, based on the scenario presented to respondents, the question regarding experience is now focused on the (biometric) recognition technology presented in this scenario. This same line of reasoning now applies in the questions corresponding with the constructs. Questions regarding the technology now specify the technology based on the scenario presented to the respondents. These adjustments to the survey increase the face validity and helped to ensure that respondents understand the questions and can relate to them as well.

Second iteration

Based on incremental insights, several changes to the questionnaire were implemented:

- In the section regarding demographic characteristics of respondents, the question concerning 'age' has been changed from categorical answers, to raw data input of the exact age. As a result, the limitations of categorical data were lifted, thus enabling more statistical analysis options.
- In the initial version, the questionnaire included a question related to the experience with the technology. However, another important factor is whether the respondent is familiar with conducting financial activities using a mobile device. Therefore, a question related to this experience has been implemented.
- Due to haziness related to the statements addressing Lifestyle Compatibility, and in particular due to the term 'Lifestyle' we decided to use different statements. Hence, instead of two (out of three) questions focusing on lifestyle, we used a new source to adapt a total of five statements to answer this construct. [22] From which four are more focused on the technology and the application itself, instead of the so-called "lifestyle".
- Due to the discovery of a mistake made during the first survey design and validation iteration, we have included more statements in the construct "Perceived Ease of Use". Instead of the three incorporated in the first version, we have adapted every statement originating from Davis' research (a total of five, excluding one statement due to remarks by the pilot test participants). [27]
- Based on remarks regarding the transactions value and question related to

the amount respondent would be willing to authorize using the technology, we changed this question to: Would you, regardless of the amount, be willing to use this technology to confirm payments?

This new version of the survey was tested using the same structure as the first iteration. Thus, by having one-on-one session with participants of a focus group (N=10; male = 6, female = 4) varying in age from 23 to 59, valuable feedback and insights were obtained. A few points were related to the function of the survey; some paths were incorrect and needed to be adjusted. Furthermore, the field in which respondents could provide their age, was not limited to only digits (a maximum of three) and no decimals. Furthermore, the important information included in the scenario description has been turned to a bold font in order to draw the attention and emphasize the recognition technology and value of the financial transaction.

Third iteration

The final iteration to test the survey was conducted by distributing the survey to a larger group of respondents. A total of 34 respondents participated ranging in age from 23 to 59 (female = 8, male = 26). A brief analysis of this data indicates that there are no routing issues in the survey, nor any unanswered questions. However, based on multiple recommendations we have deleted a part of the introduction which explained the overall structure of the survey. This was considered as superfluous and did not provide important information. Furthermore, the question related to the experience respondents have with the recognition technology has been supplemented with two other answer options. Motivation for this decision is the remark by multiple respondents that they did use this technology in the past, but not anymore, or that they had heard of it, but have not used it. Although this iteration had the sole purpose of testing the survey and its resulting data, it does show some interesting insights into the preferences of certain technologies.

3.3 Sample and respondents

The sample of our research, which was divided in six different respondent groups, reflects individuals that utilize services provided by banks or payment service providers. As aforementioned, the respondents (N = 220) were reached via online platforms and social media. For a more detailed description of the demographic characteristics of this group, see table 3.2.

Demographic characteristics respondents

	Scenario 1	*Scenario 2*	*Scenario 3*	*Scenario 4*	*Scenario 5*	*Scenario 6*	***Total***
Age							
<18	0.0	0.0	0.0	0.0	0.0	0.0	0.0
18 $\leq$ 24	22.9	30.8	20.0	14.6	21.1	18.4	21.8
25 $\leq$ 34	45.7	51.3	57.1	17.2	63.2	47.4	52.7
35 $\leq$ 44	17.1	7.7	5.7	9.1	7.9	10.5	10.0
45 $\leq$ 54	5.7	5.1	11.4	26.7	2.6	10.5	6.8
55 $\leq$ 65	2.9	5.1	5.7	11.8	5.3	13.2	7.7
>65	5.7	0.0	0.0	0.0	0.0	0.0	0.9
Gender							
Male	74.3	56.4	77.1	62.9	71.1	65.8	67.7
Female	25.7	41.0	22.9	34.3	28.9	34.2	31.4
Other	0.0	2.6	0.0	2.9	0.0	0.0	0.9
Education level							
High school	14.3	2.6	8.6	8.6	5.3	10.5	8.2
MBO	8.6	15.4	2.9	17.1	10.5	10.5	10.9
HBO	14.3	23.1	25.7	17.1	21.1	21.1	20.5
University bachelor	11.4	7.7	14.3	17.1	15.8	15.8	13.6
University master	51.4	51.3	42.9	40.0	47.4	42.1	45.9
PhD	0.0	0.0	5.7	0.0	0.0	0.0	0.9

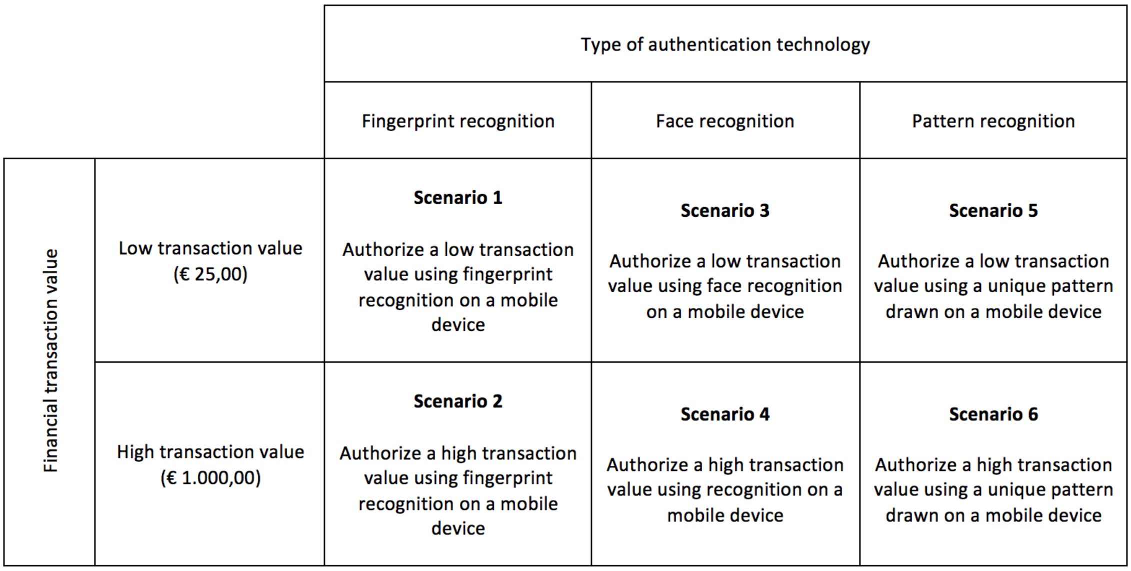
Table 3.2: Demographic characteristics of the sample groups (numbers are in percentages

3.4 Scenario design

In addition to the differences between the three recognition technologies, we are also interested in the different perceptions regarding the technologies in relation to different transaction values. Based on the perception of risk (e.g. financial risk [11]) and the fear of loss (loss aversion [55]) we predict that consumers might be more reluctant to use (biometric) recognition technologies in case of high value transactions. An example of this line of reasoning is as follows: As research indicates, consumers perceive services as more risky due to the higher levels of uncertainty associated with them in comparison to products. [81] With this uncertainty and loss aversion in mind, the consumer would like to reduce the risk. Therefore, if the amount (transaction value) at stake is higher, so is the risk. Hence, our assumption that with higher transaction values, and thus amounts of risk, individuals would be less willing to adopt a technology if they are not certain about the security and/or outcome.

To define the values of low and high value financial transactions, an investigation regarding the current limits has been conducted. In the current financial landscape of The Netherlands, wireless (NFC) payments using a debit card without providing a PIN have a limit of 25 euros. After several attempts below this amount, or in case of a higher transaction value, a different authentication is required. Based on this method, we have set the low transaction value at a value of 25 euros. To validate whether this is a reasonable assumption, participants of the pilot test (first iteration) were asked if they agreed with this limit being considered as a low value purchase. Thus, based on the current limit and confirmation of participants, the total (low) amount of 25 euros was established.

A high purchase amount, one for which you consider your options and are aware of the pros and cons of the product you are going to buy, has been established at 1.000 (thousand) euros. It can generally be assumed that purchases with this value take some time to consider and consumers will be more inclined to do some research prior to their purchase.



		Type of authentication technology		
		Fingerprint recognition	Face recognition	Pattern recognition
Financial transaction value	Low transaction value (€ 25,00)	**Scenario 1** Authorize a low transaction value using fingerprint recognition on a mobile device	**Scenario 3** Authorize a low transaction value using face recognition on a mobile device	**Scenario 5** Authorize a low transaction value using a unique pattern drawn on a mobile device
	High transaction value (€ 1.000,00)	**Scenario 2** Authorize a high transaction value using fingerprint recognition on a mobile device	**Scenario 4** Authorize a high transaction value using recognition on a mobile device	**Scenario 6** Authorize a high transaction value using a unique pattern drawn on a mobile device

Figure 3.1: Scenario description

We have designed the scenarios using previous research by Miltgen et al. and Huys as a guideline and tested the first design for bias and potential uncertainties. [43, 72] The scenarios (illustrated in Appendix A) are focused around the objective of ordering a product online and immediately authorize the payment. We have chosen for this setting due to the increasing popularity of mobile commerce (m- or e-commerce) where Pham et. al even call it *"the most important trend reshaping the retail landscape. [81, p. 159]"*. This was done with a small group of volunteers who were asked to read the scenario and then asked if they could describe their interpretation. Since these interpretations matched the goal we had in mind, no changes to the scenario description were required and the six scenarios were established (see figure 3.1).

3.5 Data preparation

The questionnaire (see appendix C) was initially distributed on the 21st of September 2018 via a variety of electronic channels (LinkedIn and Facebook). During a period of six weeks, respondents were able to follow the link and complete the survey. In this period a total of 220 respondents have completed the survey and due to built-in validation, all responses were suitable for the initial further analysis. Hence, the data was exported to IBM's SPSS 25 and AMOS and consequently adjusted before any further analyses were executed.

While loading the data into SPSS, certain columns deemed irrelevant for the goal of our research were deleted (e.g. duration of completion, date of completion, name of the respondent, and location). Regarding the data preparation, multiple steps were performed. First, all variables were renamed and labeled for better understanding during analysis (for an overview of the used names and labels, see the codebook provided in appendix C table 7.1).

The first step after relabelling and renaming the variables, was to dummy code several variables. First, the variables 'Technology' (0=; Fingerprint; 1= Facial; 2=Pattern) and 'Amount' (0 = Low; 1 = High) were dummy coded. Second, we adjusted the measurement scale of every variable to the correct one (e.g. ordinal, nominal or scale). The following adjustment consisted of reverse coding a total of four items (Innov3, PPC2, PPC3, and PPC4). This step was required due to the negative/positive wording of these questions, hence making sure the responses fit the other scales. Fifth, as a consequence of the specification of questions based on the described technology, we had to dummy code the questions not presented to respondents. Thus, questions adjusted to a illustrated technology not presented to respondents were dummy coded (0 = not shown to respondent due to scenario). This alteration of the data enabled further calculations such as calculation the mean and total in one single column, despite the scenarios presented to respondents. Following this step, we used SPSS' compute function to calculate total scores and means for constructs as well as item totals and means across technologies and price levels. It should be mentioned that all computations and transformations of variables leading to alterations in the data, were recorded as new variables. Thus, enabling the traceability and preventing the loss of data.

3.6 Analytical procedure

Before proceeding with the tests that will enable us to answer the hypotheses and research questions, several preliminary tests were executed.

First of all, we wanted to make sure that the demographic characteristics in each group were more or less equal. Thus, we executed a one-way ANOVA to test whether there was a significant difference between the six groups (one group for every scenario). As shown in table 3.3, it was found that, based on the demographic characteristics age, gender, and education level, there are no significant differences in the population means. Hence, the null hypothesis cannot be rejected. This result allows us to draw conclusions that do not have to take into account a difference between scenarios based on a varying demographic buildup regarding the respondents of that group. Although this study faces a lack of respondents in the older age categories, this does not affect the demographic built-up of the six sample groups.

However, the control variable 'Experience' does differ significantly, hence we performed Tukey's HSD post-hoc test. This test shows that there is a difference between scenarios 1 and 4, scenarios 2 and 4, and scenarios 4 and 5. This difference makes sense since scenarios 1 and 2 use the same technology (fingerprint recognition), just like 3 and 4 (facial recognition), and 5 and 6 (pattern recognition). Thus, control effects for the variable 'Experience' should be interpreted carefully.

ANOVA

		Sum of Squares	*df*	*Mean Square*	*F*	*Sig.*
Age	Between Groups	832.516	5	166.503	1.220	.301
	Within Groups	29196.734	214	136.433		
	Total	30029.250	219			
Gender	Between Groups	.596	5	.119	.510	.768
	Within Groups	49.999	214	.234		
	Total	50.595	219			
Education level	Between Groups	3.288	5	.658	.351	.881
	Within Groups	400.694	214	1.872		
	Total	403.982	219			
Experience	Between Groups	9.461	5	1.892	3.613	0.004
	Within Groups	112.085	214	.524		
	Total	121.545	219			

Table 3.3: Results of one-way ANOVA analysis

Following the one-way ANOVA analysis, we used a Pearson correlation matrix to test if variables, either independent, dependent or control variables, showed any correlation. As indicated by the correlation matrix (presented in table 3.4), there are significant correlations between the variables on both the 0.05 and 0.01 level (2-tailed).

	Mean	S.D.	Gender	Age	Ed. lvl	Innov	Tech. Exp.	MB. Exp.	Rec. Tech.	TV	LC	PR	PPC	PS	PEoU	BI
Gender	.70	.48	1													
Age	32.25	11.71	-.051	1												
Edu LvL	2.81	1.36	.022	-.289**	1											
Innovativeness	4.70	1.22	.218**	-.144*	.174**	1										
Technology exp.	.95	.74	.127	-.371**	.145*	.165*	1									
M-banking exp.	.09	.28	-.041	.244**	-.076	-.159*	-.155*	1								
Recognition Technology	1.01	.83	.007	.012	-.015	.004	-.066	.095	1							
Transaction value	.50	.51	-.093	.065	-.051	-.160*	-.048	.075	-.022	1						
Lifestyle Compatibility	4.56	1.62	-.114	-.133*	.171*	.141*	.282**	-.285**	.344**	-.095	1					
Perceived Risk	4.11	1.29	.010	.088	-.237**	-.181**	-.189**	.246**	.188**	.115	-.438**	1				
Perceived Privacy Concern	3.51	1.04	-.036	.153*	-.155*	-.314**	-.251**		.082	.225**	-.426**	.601**	1			
Perceived Security	4.19	1.42	-.078	0,030	0,051	0,107	.233**	-.188**	-.358**	-.067	.740**	-.480**	-.413**	1		
Perceived Ease of Use	6.13	.87	.094	-.302**	.215**	.203**	.356**	-.205**	-.073	-.135*	.355**	-.273**	-.398**	.273**	1	
Behavioral Intention	4.28	1.93	-.098	-.059	.167*	.073	.301**	-.232**	-.435**	-.094	.816**	-.473**	-.416**	.784**	.348**	1

$^{*}p < 0.05$, $^{**}p < 0.01$ (2-tailed)

Table 3.4: Pearson correlation matrix

Due to the describing nature of multiple variables in order to test theory (hypotheses) the most suitable way for us to test our model is by Structural Equation Modeling (SEM). This point is strengthened by Schumacker and Lomax who state: "*SEM techniques are therefore becoming the preferred method for confirming (or disconfirming) theoretical models in a quantitative fashion. [67, p. 7]*" By using SEM we are able to use multiple variables and identify direct and indirect effects. The second advantage of using this technique, is that it enables us to use multiple indicators of a single concept (the items in relation to the constructs). [105]

The way in which we apply SEM, by using IBM's AMOS software, is to create a model that illustrates the conceptual model illustrated in figure 2.10. AMOS' latent and observed variables allows us to model exactly the items and constructs included in our research framework. Thus, the individual answers to the questions of the survey are used as input for the observed variables (the items). These variables, or items, are then combined to measure the latent variables (the constructs). However, before we are able to use this model for the analysis regarding the relations between the constructs, it must be tested whether the model is correct.

To test whether a model is correct can be done using AMOS. In Confirmatory Factor Analysis (CFA) we test a model using multiple model-fit criteria and the maximum likelihood estimator. When this test is conducted we will identify if these meet the criteria proposed by Lomax and Schumacker, or if some adjustments are required. From the executed CFA we can conclude that our model has a good model fit (chi-square = 823.388 ; df = 496 ; p-value = .000). While this p-value is non-significant, the power of this indicator reduces at samples consisting of about 200 respondents. Therefore, the remaining indicators of model fit (NFI. TLI, IFI, CFI, and RMSEA) are used to identify our model fit.

With a Tucker-Lewis Index (TLI) of .928 the model exceeds the criteria of .90, thus having a good model fit according to this indicator. The following criteria, the Normal Fit Index (NFI), falls just short of .90 with a score of .863. However, this minor difference is deemed acceptable since the other criteria are met. Both the Incremental Fit Index (IFI), and Comparative Fit Index (CFI), exceed their criteria of .90 with scores of .941 and .940 respectively. Lastly, our score for Root Mean Square Error of Approximation (RMSEA) is .055, which is slightly higher than the .05 criteria. All in all, we can conclude that our overall model has good global fit. [67] For the graphical illustration of the CFA model, see appendix E.

As shown in table 3.5, the found composite reliability of every single construct exceed the threshold of .7 and thus is found to be acceptable. Hence, the internal consistency of the constructs will not cause any issues during further analysis. To test discriminant validity, the average variance extracted (AVE) has been calculated. All constructs, except Perceived Privacy Concern exceed the suggested threshold of .5 [33]. It can be concluded that the values obtained indicate adequate internal consistency reliability and convergent validity.

Finally, we executed Harman's one-factor test to address the possibility of common method bias using the IBM's software 'SPSS 25'. With all items incorporated in this test, the results indicated that six factors accounted for 71.8% of the variance. The largest single factor contributed to this variance with a total of 36.5%. Thus, while not indicating the presence or absence, it can be concluded that the results of our study are not affected by the common method bias. [82]

Construct	**Item**	**Mean**	**S.D.**	**Factor loading**	**AVE**	**CR**
Lifestyle Compatibility	LC1	4.70	1.751	.883	.766	.942
	LC2	4.51	1.869	.923		
	LC3	4.58	1.884	.932		
	LC4	4.35	1.712	.668		
	LC5	4.69	1.825	.939		
Perceived Ease of Use	PEoU1	6.09	1.115	.723	.716	.926
	PEoU2	6.19	.881	.779		
	PEoU3	6.10	.994	.917		
	PEoU4	6.16	1.007	.919		
	PEoU5	6.08	.942	.876		
Perceived Risk	PR1	5.02	1.503	.753	.548	.824
	PR2	3.68	1.579	.491		
	PR3	3.50	1.705	.789		
	PR4	4.26	1.669	.873		
Perceived Privacy Concern	PPC1	3.78	1.808	.536	.325	.707
	REC_PPC2	4.71	1.413	.595		
	REC_PPC3	5.14	1.174	.588		
	REC_PPC4	4.54	1.518	.582		
	PPC5	4.17	1.601	.549		
Perceived Security	PS1	4.54	1.623	.569	.556	.830
	PS2	3.94	1.640	.700		
	PS3	4.45	1.836	.883		
	PS4	3.85	1.784	.793		
Behavioral Intention	BI1	4.20	1.992	.989	0.924	0.973
	BI2	4.15	2.002	.984		
	BI3	4.49	1.957	.908		
Innovativeness	Innov1	4.62	1.517	.833	.552	.827
	Innov2	4.00	1.681	.815		
	REC_Innov3	4.95	1.507	.509		
	Innov4	5.21	1.377	.771		

Table 3.5: Overview of constructs and items with their loadings, AVE and CR

Chapter 4

Results

4.1 Direct relations

To discover the effect(s) of the different variables on the Behavioral Intention of customers, a multiple linear regression (ML) analysis was executed (see table 4.2 for the results). This analysis was divided in three different models:

- The first model looks at the association between the independent variable (IV) 'Lifestyle Compatibility' and the dependent variable (DV) 'Behavioral Intention'.
- The second model entails the association between the IV and the four constructs Perceived Ease of Use (PEoU), Perceived Risk (PR), Perceived Privacy Concern (PPC), and Perceived Security (PS).
- Lastly, model three looks at the associations between the IV and DV, while controlling for (potentially) mediating constructs.

Based on the results of the executed MLR (illustrated in table 4.2), it was found that in the first model the IV 'Lifestyle Compatibility' is significantly and positively associated with BI ($\beta = .787, p < 0.0001$). In the third model, while incorporating the potentially mediators, the independent variable LC, was still found to be significantly and positively associated with the DV Behavioral Intention ($\beta = .480, p < 0.0001$). This confirms hypothesis $H1_a$ in both models.

The second model, which incorporates the associations between the independent variable LC and the dependent variables PEoU, PR, PPC, and PS shows multiple significant associations. First of all, the results indicate a significant and positive association between LC and PEoU ($\beta = .277, p < 0.0001$) confirming hypothesis $H2_a$. Second, the association between LC and PR is found to be significant and negative ($\beta = -.400, p < 0.0001$) confirming hypothesis $H4_a$. Third, the association between LC and PPC was found to be significant and negatively associated ($\beta = -.388, p < 0.0001$). Which confirms hypothesis $H6_a$. Finally, the association between LC and PS was found to be significant and positive ($\beta = .744, p < 0.0001$) confirming hypothesis $H8_a$.

Lastly, in model three, where we tested the effect of LC and the mediating effects of the four other variables on the DV Behavioral Intention, showed two significant associations. As aforementioned the first significant and positive association, is that between LC and BI ($\beta = .480, p < 0.0001$). Second, a significant and positive association was found between Perceived Security and Behavioral Intention ($\beta = .368, p < 0.0001$). Hence, we can conclude that hypothesis $H9$ is confirmed in model 3 while rejecting hypotheses 3, 5, and 7.

Hypothesis		**Conclusion**	**Argument**
1	a	Confirmed	-
	b	Rejected	No significance
2	a	Confirmed	-
	b	Rejected	No significance
3		Rejected	No significance
4	a	Confirmed	-
	b	Rejected	No significance
5		Rejected	No significance
6	a	Confirmed	-
	b	Rejected	No significance
7		Rejected	No significance
8	a	Confirmed	-
	b	Rejected	No significance
9		Confirmed	-

Table 4.1: Results hypotheses testing

	Model 1			**Model 2**												**Model 3**		
Dependent variables	Behavioral Intention			Perceived Risk			Perceived Privacy Concern			Perceived Security			Perceived Ease of Use			Behavioral Intention		
	B (SE)	β	t-value	B (SE)	β	t-value	B (SE)	β	t-value	B (SE)	β	t-value	B (SE)	β	t-value	B (SE)	β	t-value
Control variables																		
Age	.017 (.012)	.102	1.438	-.004 (.008)	-.041	-.559	.003 (.006)	.039	.530	.018 (.009)	**.149***	2.053	-.012 (.005)	**-.162***	-2.350	.017 (.012)	.102	1.438
Gender	-.558 (.257)	**-.139***	-2.170	.095 (.177)	.035	.537	-.009 (.143)	-.004	-.060	-.323 (.195)	-.109	-1.660	.089 (.113)	.049	.783	-.558 (.257)	**-.139***	-2.170
Education level	.215 (.094	**.151***	2.279	-.213 (.065)	**-.224*****	-3.281	-.086 (.053)	-.112	-1.634	.057 (.071)	.054	.795	.082 (.041)	**.128***	1.974	.215 (.094)	**.151***	2.279
Experience	.867 (.179)	**.334******	4.850	-.306 (.123)	**-.176****	-2.490	-.308 (.099)	**-.220****	-3.096	.561 (.135)	**.294******	4.150	.318 (.079)	**.271******	4.044	.867 (.179)	**.334******	4.850
R^{2} (adjusted)	.133 (.117)			.083 (.066)			.079 (.061)			.084 (.067)			.178 (.162)			.133 (.117)		
F	**8.275******			**4.883*****			**4.585*****			**4.940*****			**11.614******			8.275****		
Moderator																		
Innovativeness	.015 (.037)	.016	.401	.025 (.038)	.040	.653	.038 (.031)	.076	1.229	.020 (.031)	.029	.639	-.050 (.025)	**-.119***	-1.972	.012 (.033)	.013	.350
Independent variables																		
Lifestyle Compatiblity	.938 (.049)	**.787******	19.043	-.319 (.051)	**-.400******	-6.227	-.249 (.042)	**-.388******	-5.999	.653 (.042)	**.744******	15.586	.149 (.034)	**.277******	4.401	.572 (.066)	**.480******	8.724
Perceived Ease of Use																.110 (.092)	.049	1.196
Perceived Risk																-.089 (.070)	-.059	-1.274
Perceived Privacy Concern																.021 (.086)	.011	.247
Perceived Security																.500 (.075)	**.368******	6.655
R^{2} (adjusted)	.680 (.671)			.225 (.203)			.215 (.193)			.757 (.573)			.257 (.236)			.750 (.738)		
ΔR^2	**.554**			.137			.132			.506			.074			.621		
F	**362.626******			**38.779******			**35.990******			**242.913******			**19.368******			**102.640******		

$^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$, $^{****}p < 0.0001$ (2-tailed)

Table 4.2: Results multiple linear regression analysis

4.2 Moderation analysis

In our conceptual model, we hypothesized the existence of a moderating variable 'Innovativeness' on the relations between the IV 'Lifestyle Compatibility' and the constructs PR, PPC, PS, and PEoU, and on the relation between LC and the DV 'Behavioral Intention'. As stated by Baron and Kenny: "*... a moderator is a qualitative or quantitative variable that affects the direction and/or strength of the relation between an independent or predictor variable and a dependent or criterion variable. [14, p. 1174]*"

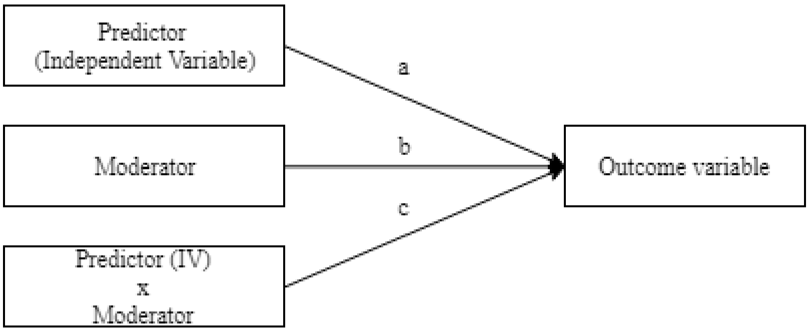


Figure 4.1: Moderator path diagram [14, p. 1174]

After executing multiple moderation tests, one significant interaction effect was found. As the multiple linear regression table shows (see table 4.2), innovativeness appears to be a significant moderator on the association between LC and PEoU ($\beta = -.119, p < 0.05$). However, since the association is negative, hypothesis $H2_b$ is rejected. Moreover, since the moderation of this association is the only one showing significant results, all other hypotheses ($H1_b$, $H4_b$, $H6_b$, and $H8_b$) that incorporate the moderating effect of 'Innovativeness' have to be rejected.

4.3 Mediation analysis

Before identifying the mediation effects in our study, it should be mentioned that Baron and Kenny describe two types of mediation: partial and full mediation. In order to identify mediation effects in our model, we applied the conditions advocated by Baron and Kenny [106, 14]. To test for mediation effects, we applied the three linear regression equations advocated by Baron and Kenny. Hence, the following regressions were applied to the data [14]:

1. Regressing the mediator on the IV
2. Regressing the IV on the DV
3. Regressing the DV on both the mediator and IV

The aforementioned conditions of mediation are: (1) there is a significant relationship between the independent (IV) and suspected mediator (M). (2) The variations in M are significant related to the DV. (3) When controlling for paths a and b, the previously significant relation between the IV and DV are no longer significant. In this case, when path c is zero it is considered to be the strongest demonstration of mediation. If the affect decreases but is still not equal to 0, then partial mediation is exhibited. [106, 14, p. 555]

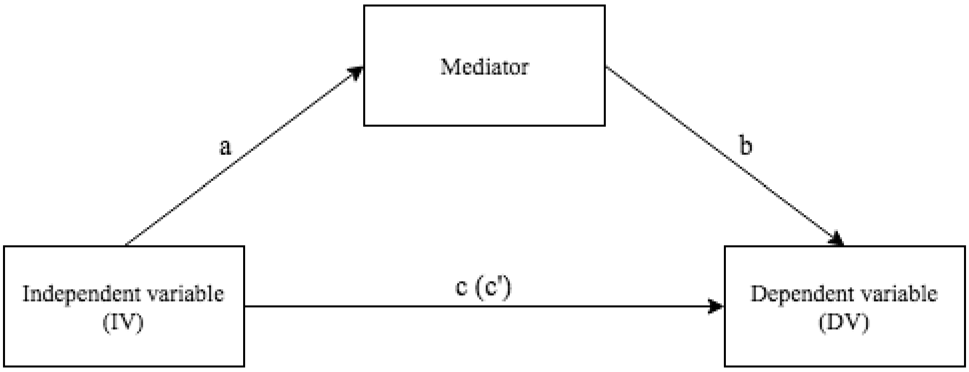


Figure 4.2: Mediator diagram [14, p. 1176]

As presented in table 4.3, two of the four constructs were found to have mediating effects. In this study, Perceived Risk and Perceived Security were found to have a partial mediating effect on the associations between Behavioral Intention and Lifestyle Compatibility.

IV	*Mediator*	*c-path*	*a-path*	*b-path*	*c'-path*	*Type of mediation*
Lifestyle Compatibility	Perceived Ease of Use	$.787^{***}$	$.277^{***}$	.071	$.768^{***}$	No mediation
	Perceived Risk	$.787^{***}$	$-.400^{***}$	$-.136^{**}$	$.733^{***}$	Partial
	Perceived Privacy Concern	$.787^{***}$	$-.388^{***}$	-.080	$.756^{***}$	No mediation
	Perceived Security	$.787^{***}$	$.744^{***}$	$.392^{***}$	$.495^{***}$	Partial

DV = Behavioral Intention, ${}^{*}p < 0.05$, ${}^{**}p < 0.01$, ${}^{***}p < 0.001$ (2-tailed)

Table 4.3: Results of mediation analysis

4.4 Control variables

Resulting from the multiple linear regression analysis, several significant associations were found between the control variables and the dependent variables. Closer examination of the variables shows that age is significantly and negatively associated with Perceived Security ($\beta = -.149, p < 0.05$) and Perceived Ease of Use ($\beta = -.162, p < 0.05$). These results indicate that younger individuals perceive the technology as more secure (or safer) and easier to use. In contrast, older individuals tend to be more negative about the security of the technology and its ease of use. However, as mentioned before and further elaborated in the limitations, due to lack of a sufficient number of responses in the oldest age group, conclusions regarding age should be interpreted with caution.

The results for the control variable 'gender' indicate that it is significantly and negatively associated with Behavioral Intention ($\beta = -.139, p < 0.05$). Thus, for this variable the findings suggest that females have a higher Behavioral Intention than men. Moreover, after examination of other significant control variables, the findings suggest that education level is significantly and positively associated with Behavioral Intention ($\beta = .151, p < 0.05$) and Perceived Ease of Use ($\beta = .128, p < 0.05$). Indicating that for individuals who have obtained degrees in higher education and academia, their BI and PEoU are more positive (or higher). Furthermore, education level is significantly and negatively associated with Perceived Risk ($\beta = -.224, p < 0.001$). This suggests that having followed and completed higher education, one has a lower perception of risk associated to the scenario presented to the individual.

Lastly, experience with the technology appears to be significantly associated with all other variables. Experience is significantly and positively associated with BI ($\beta = .334, p < 0.0001$), PS ($\beta = .294, p < 0.0001$), PEoU ($\beta = .271, p < 0.0001$). Moreover, two significant negatively associations were found between experience and PR ($\beta = -.176, p < 0.001$) and between experience and PPC ($\beta = -.220, p < 0.001$). These results indicate that for BI, PS and PEoU, having more experience with the technology results in a positive perception of these variables. Likwise, the more experienced individuals perceive the technology as less risky and worry less about the privacy related aspects.

4.5 Scenario comparisons

In addition to the identification of the associations in our model, and corresponding hypotheses, the main goal of this study is to compare a set of technologies and the dichotomy of low and high value transactions. To identify differences between the scenarios regarding the Lifestyle Compatibility, Perceived Risk, Perceived Privacy Concern, Perceived Security, Perceived Ease of Use, and Behavioral Intention, we applied a one-way ANOVA analysis. The results of this analysis, using the construct variables as the dependent list and the scenario variable as the factor, are presented in table 4.4.

Table 4.4 shows the results of the executed one-way ANOVA used to test for differences between the construct means among the six different respondent groups. As discussed in paragraph 3.6, the null hypothesis that there are no significant differences in the scenario means for the constructs cannot be rejected for Perceived Ease of Use (PEoU), thus there appears to be no difference between the technologies regarding their PEoU. In contrast, the constructs Lifestyle Compatibility (LC), Perceived Risk (PR), Perceived Privacy Concern (PPC), Perceived Security (PS), and Behavioral Intention (BI), are significant. Thus, the null hypotheses can be rejected since there are significant differences among the means of the constructs (varying from the 0.05 level to the 0.001 level).

To achieve our goal regarding the comparison of the six scenarios based on the presented technologies and transaction values, a one-way ANOVA analysis has been executed. The results of this test show that in case of the constructs 'Lifestyle Compatibility', 'Perceived Risk', 'Perceived Privacy Concern', 'Perceived Security', and 'Behavioral Intention' significant variations were discovered. Since the ANOVA analysis does not specificy these variations for every scenario, Tukey's post-hoc test has been executed. The results of this test will be discussed in the following paragraphs. However, it should be mentioned that the results of the mean difference between I (the first scenario in the Tukey test) and J the second scenario in the Tukey test) will be used to discuss the differences between scenarios, and hence, technologies and price levels.

ANOVA

		Sum of squares	*df*	*Mean Square*	*F*	*Sig.*
Lifestyle Compatibility	Between groups	841.491	5	16.898	7.367	**.000******
	Within groups	490.873	214	2.294		
	Total	575.363	219			
Perceived Risk	Between groups	21.726	5	4.345	2.711	**.021***
	Within groups	343.058	214	1.603		
	Total	364.784	219			
Perceived Privacy Concern	Between groups	23.793	5	4.759	4.761	**.000******
	Within groups	213.886	214	.999		
	Total	237.679	219			
Perceived Security	Between groups	63.300	5	12.660	7.137	**.000******
	Within groups	379.580	214	1.774		
	Total	442.880	219			
Perceived Ease of Use	Between groups	6.277	5	1.255	1.678	.141
	Within groups	160.090	214	.748		
	Total	166.367	219			
Behavioral Intention	Between groups	176.318	5	35.264	11.768	**.000******
	Within groups	641.249	214	2.996		
	Total	817.568	219			

$^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$, $^{****}p < 0.0001$

Table 4.4: Results of scenario comparison (one-way ANOVA)

Lifestyle Compatibility

As indicated by the ANOVA analysis, significant variations between the scenarios were found for the construct 'Lifestyle Compatibility'. Closer examination of the results from Tukey's HDS post-hoc test indicate that using fingerprint recognition to authorize low transaction value differs from facial recognition with both a low (mean difference I-J = 1,29; p = .006), and high transaction value (mean difference I-J = 1,35; p = .003). Furthermore, fingerprint recognition for the authorization of low transaction values differed from both low, and high transaction values authorized using pattern recognition (mean difference I-J = 1,34; p = .003 and mean difference I-J = 1,83; p = .000 respectively).

In addition to variations from the first scenario, scenario 2 (fingerprint recognition with a high transaction value) was found to vary from scenario 6 (pattern recognition with a high value transaction: mean difference I-J = 1,39; p = .001).

Perceived Risk

Perceived Risk was found to differ significantly between scenarios: Scenario 1 differed from scenario 4 which represented using facial recognition to authorize transactions with a value of 1.000 euros (mean difference I-J = -.900; p = .038). Moreover, scenario 1 differed from scenario 6 which represented using pattern recognition to authorize transactions with a value of 1.000 euros (mean difference I-J = -.950; p = .019).

Perceived Privacy Concern

Perceived Privacy Concern was found to differ significantly between scenarios: First, scenario 1 differed from scenario 4 (mean difference I-J = -1.08; p = .000). Second, scenario 1 was found to differ from scenario 6 (mean difference I-J = -.731; p = .025). Lastly, scenario 4 was found to differ from scenario 5 (mean difference I-J = .739; p = .022).

Perceived Security

As indicated by the ANOVA test, this construct is found to significantly differ between scenarios. First, scenario 1 differs from scenario 3 (mean difference I-J = .986; p = .027) and scenario 4 (mean difference I-J = 1.17; p = .004) Second, scenario 1 differs from scenario 5 (mean difference I-J = 1.43; p = .000) and scenario 6 (mean difference I-J = 1.47; p = .000). Moreover, scenario 2, the fingerprint recognition technology in combination with a high value transaction is found to be significantly different from scenario 5 (mean difference I-J = 1.01; p = .013) and scenario 6 (mean difference I-J = 1.05; p = .008).

Behavioral Intention

Behavioral Intention was found to differ significantly between multiple scenarios. First of all, BI was found to differ between scenario 1 and scenario 3 (mean difference I-J = 1.68; p = .001). Second of all, Scenario 1 differed from scenario 4 (mean difference I-J = 1.90; p = .000) Third of all, scenario 1 and scenario 5 (mean difference I-J = 2.01; p = .000). And lastly, scenario 1 and scenario 6 (mean difference I-J = 2.54; p = .000).

Furthermore, scenario 2 was found to significantly differ from: scenario 3 (mean difference I-J = 1.17; p = .048), scenario 4 (mean difference I-J = 1.38; p = .009), scenario 5 (mean difference I-J = 1.56; p = .002), and scenario 6 (mean difference I-J = 2.03; p = .000).

Chapter 5

Discussion

After gathering the data that was generated during the six weeks in which the questionnaire was available to respondents, a variety of analysis were executed. First of all, an ANOVA analysis was used to indicate the variations between the scenarios regarding demographic details of respondents (illustrated in table 3.3). This analysis indicated no significant differences related to age, gender, or education level among the respondents of the sample groups. Experience however was found to differ significantly; this makes sense since some technologies are more common and have been on the market for a longer period of time (pattern recognition) than others (e.g. fingerprint, and facial recognition).

Following the one-way ANOVA, we used IBM's AMOS software to perform a Confirmatory Factor Analysis (CFA; illustrated in figure 7.5 in Appendix E) which showed acceptable levels of AVE and CR, thus indicating discriminant validity and internal consistency and acceptable factor loadings (presented in table 3.5).

5.1 Multiple linear regression

After proving the reliability and validity of the data, a multiple linear regression has been executed (see table 4.2). This analysis indicated the significance of Lifestyle Compatibility as a predictor of Perceived Ease of Use, Perceived Risk, Perceived Privacy Concern, Perceived Security, and Behavioral Intention. From these results it can be concluded that individuals who have the opinion that a technology fits their lifestyle will find the technology easier to use, and more secure while at the same time are less worried about their privacy being violated and perceive a lower risk perception.

In contrast, individuals who do not share this positive opinion about the technology fitting their lifestyle, have a different view of these constructs. A lower score of LC will result in higher degrees of Perceived Risk and Perceived Privacy Concern, lower scores of Perceived Security, Perceived Ease of Use, and Behavioral Intention.

The hypothesized moderating effect of innovativeness was found to be significant in one particular case; the association between LC and PEoU. However, the expected moderating result was the opposite of the actual outcome; instead of a stronger positive result in case of higher innovativeness scores, the opposite was proven. The effect of LC on PEoU was weaker when the individual has a higher innovativeness score.

In conclusion, individuals who perceive the technology as compatible with their lifestyle will have a more positive opinion regarding the presented technology, its security, ease of use, and have a greater intention to use (biometric) recognition technologies on mobile devices for the authorization of financial transactions.

5.2 One-way ANOVA scenario comparison

Resulting from the prior one-way ANOVA and Tukey's HSD post-hoc test, several variations between the constructs in every scenario were found. We will further elaborate on these results and discuss them in the following paragraphs.

Scores for the LC construct were found to vary between scenario 1 and scenarios: 3, 4, 5, and 6. This indicates that using fingerprint recognition for the authorization of transactions with a low value is a significantly better fit to the lifestyle of respondents than the other scenarios and transactions with a high value. Moreover, scenario 2 was found to significantly differ from scenario 6. This result indicates that in case of transactions with a high value, respondents prefer to use fingerprint recognition over pattern recognition. Perhaps most interesting, is that regarding transaction with a high value, the LC does not differ significantly between face recognition and pattern recognition.

For the construct 'Perceived Risk', scores were found to significantly vary between scenario 1 and scenario 4 and 6. This result indicates that using fingerprint recognition to authorize a transaction with a low value was perceived as 'least risky' while significantly differing from the two other technologies, however, only when regarding the transactions with a high value. Apparently, the value of the transaction did not differ for fingerprint recognition technology or the other technologies in case of transactions with a low value.

Perceived Privacy Concern, was found to be significantly different between scenario 1 and scenarios 4 and 6. Thus, indicating that individuals were more concerned about their privacy in case of transactions with a high value using either face recognition or pattern recognition. Furthermore, scenario 4 was found to differ from scenario 5, indicating that individual were more concerned in case of using face recognition for authorising a transaction with a high value when compared to a transaction with a low value using pattern recognition.

The construct 'Perceived Security' is the only variable besides LC that was found to be a predictor to Behavioral Intention in the third model. With the ANOVA and subsequently Tukey's HSD test, it was found that scenario 1 varied from scenario 3, 4, 5, and 6 while scenario 2 differed from scenario 5 and 6. These results indicate that using fingerprint recognition for the authorization of low value transactions was perceived as more secure compared to all other scenarios, except scenario 2. However, scenario 2 was found to be more secure when compared to both the low and high transaction value authorized using pattern recognition. In conclusion, fingerprint recognition is perceived to be the most secure authentication method for both low and high transaction values.

Respondents to the survey gave the highest BI scores to the two scenarios related to fingerprint recognition. Although the two scenarios did not differ from each other, they did differ from all other scenarios (e.g. 3, 4, 5, and 6).

5.3 Exploratory survey analysis

As discussed in chapter 3, the last part of the survey consisted of several components: a question regarding respondents' willingness to use the presented technology to authorize transactions disregarding the value of it, room for remarks, and the option to leave their contact information (see Appendix D).

From a total of 220 respondents, 60% is not willing to authorize financial transactions, disregarding the amount, using the technology presented to them in our scenarios. However, upon close examination of the individual technologies, from the respondents who were presented with fingerprint recognition (N = 74), 52.7% said they were willing to use this authentication method disregarding the value of a transaction.
From the respondents who were presented with facial recognition (N = 70), 34.3% was willing to use this authentication method disregarding the value of a transaction.

Against our expectations, from the respondents who were presented with pattern recognition (N = 76), 35.5% was willing to use this authentication method disregarding the value of a transaction. Thus, although it is perceived as less secure, there is still some degree of willingness to authorize transactions using this technology.

By studying the remarks of respondents (N = 50) is can easily be concluded that many of them realize the potential dangers of using the presented technologies. While overall, many stated that they would accept the presented technology in case of two-factor authentication (N = 14), using only the presented technology appears to be causing some negative feelings. However, using the technology for transactions up to a certain predetermined transaction value would be accepted by 18% of the respondents who left remarks (N = 9).

Furthermore, the remarks imply that many respondents who left a remark are concerned about the ease with which a third party would be able to obtain their biometric data. At the same time however, it appears that many respondents do not feel a sense of necessity regarding the usage of a different authentication method than a PIN.

Chapter 6

Conclusion

6.1 Conclusion

The aim of this study was to find an answer to the following research question:

> *"How are consumers of payment services in The Netherlands adopting mobile biometric authentication methods to authorize financial transactions?"*

In order to answer the research question, it has been divided into several manageable parts. Hence, the following sub questions were formulated:

1. Which factors contributing to consumers' Technology Acceptance are mentioned by previous research?
2. Which effect do privacy and security related constructs have on consumers' Technology Acceptance regarding biometric authentication methods on mobile devices for the authorization of financial transactions?
3. How does the Technology Acceptance of consumers differ between face recognition, fingerprint recognition, and pattern recognition?
4. How does the value of a transaction affect the perception of consumers regarding the usage of different mobile biometric authentication methods for financial transactions?

By providing answers to the sub questions and research question above, we developed new insights in the factors contributing to the Technology Acceptance of consumers. Moreover, by studying these effects regarding (biometric) recognition technology as an authentication method to authorize financial transactions using mobile devices (see paragraph 1.3), we address the research gaps as illustrated by Huys, Ogbanufe, Schierz et al, and Miltgen et al. [43, 76, 88, 72] In addition, whereas MBanking, electronic banking, and mobile payments have experienced a lot of attention within academia, the combination of e-commerce and using mobile devices as an authentication device for payments lacks attention. [25] Thus, our research explicitly fills the literature gap regarding biometric recognition technologies supported by mobile devices for the authorization of transactions.

By incorporating a total of six constructs (Lifestyle Compatibility, Perceived Ease of Use, Perceived Risk, Perceived Privacy Concern, Perceived Security, and Behavioral Intention) this study enables the discovery of variations across these constructs, consequently the effects of the type of recognition technology and transaction value on the consumer's Behavioral Intention.

Lifestyle Compatibility was found to be the most important and strongest predictor of Behavioral Intention and positive perceptions regarding the other variables. Moreover, it also indicated the best 'fit' for fingerprint recognition for transactions with both a low- and high value. Perceived Security was found to be significantly associated with Behavioral Intention, indicating that consumers prioritize security as a factor predicting if they will accept or reject a technology. Again this variable was most favorable for the two scenarios concerning fingerprint recognition.

6.2 Implications

6.2.1 Theoretical implications

From the theoretical perspective, our study has contributed to the existing Technology Acceptance literature by validating existing and adding new knowledge regarding the associations between Lifestyle Compatibility and the subsequent mentioned factors. By applying the proposed model to the context of (biometric) recognition technologies as an authentication method for the authorization of financial transactions using mobile devices, this study is the first of its kind. Using innovation diffusion, technology acceptance and innovation adoption theory as a foundation we applied our proposed conceptual model and revealed the effect of Lifestyle Compatibility, Perceived Ease of Use, Perceived Risk, Perceived Privacy Concern, and Perceived Security on the Behavioral Intention to use (biometric) recognition technologies on mobile devices.

Lifestyle Compatiblity was found to be significantly associated with the other constructs. First of all, it was found to be positively associated with Perceived Ease of Use, supporting previous studies regarding iris recognition by by Miltgen et al. [72], and a study by Koenig-Lewis et al. regarding the acceptance of mBanking. [59]

With this study we addressed calls for research by looking at the privacy and security perception of consumers. [76] Where our research looked at the Perceived Privacy Concern and Perceived Security, we found the perception of respondents in a total of 6 scenarios, with differences between them. By using the setting of mobile transaction authentication for online purchases, we also address the gap suggested by Huys, who suggested to test her research in a different setting. [43] As advocated by Lee (2009), customers' acceptance of technologies and services may be influenced by cultural factors. Thus, with our study we addressed this call by providing insights in the customers' TA only in The Netherlands, enabling comparisons of several constructs among different countries and cultures. [63]

In conclusion, this study contributes to the general understanding of the adoption of three different authentication methods, in particular the adoption of biometric authentication methods on mobile devices.

6.2.2 Practical implications

In recent years we have seen an increase in the number of PSPs, banks and other organizations who are starting to implement biometric technologies in their devices and service offerings. The results of this research support Gourville's theory in which he advocates that innovations should require low to none behavioral changes. [37] The results indicate that it is recommended for PSPs and banks to consider the details of their architecture supporting the use of these technologies as well as the awareness among customers. The preference of customers regarding fingerprint recognition could be based on their prior experience with this technology and the perception of security. An important issue regarding the practical aspects of biometric authentication is addressed by Jain et al: "*Like any other user authentication mechanism, a biometric system can be circumvented by a skillful impostor given the right circumstances and plenty of time and resources. Mitigating such concerns is essential to gaining public confidence and acceptance of biometric technology. [48, p. 88]*"

As this study indicates, it appears that the majority of the public is not aware of the safety of biometric recognition technologies as there is a certain degree of fear regarding attackers or imposters stealing their biometric template (as mentioned in several remarks by respondents). Therefore, resulting from this study we can formulate the following (business) advice:

1. As this study explored both drivers and inhibitors related to the adoption of biometric recognition technologies, organizations are encouraged to focus on the improved security when using biometric recognition technologies.
2. The value of the transaction is an important factor affecting the intention of consumers. As the gathered data and provided remarks show, consumers would like to have multiple-factor authentication, especially in case of high value transactions.
3. Remarks left by respondents indicate that a significant number of individuals are not aware of the advances in technology and corresponding security. Therefore, a striking campaign focusing on informing consumers about the security benefits provided by these technologies might prove valuable to the widespread adoption.

Furthermore, the results of our study indicate that there is a difference in perceptions when comparing the technologies, as well as the value of a transaction. Financial organizations implementing and offering biometric recognition technologies should keep the desires and opinions of consumers in mind. As our study indicates, many respondents are not willing to use either technology as the only method to authorize payments. Some advocate two-factor authentication (which is also incorporated in the PSD2) using the presented technology together with an old-fashioned PIN.

Whereas others suggest setting limits on the value authenticated using method 'X' or method 'Y'. Thus, if organizations wish to offer such authentication methods, attention should be paid to the precise limits.

6.3 Limitations

Although great consideration has been put into the design of the survey, its contents, the iterative validation cycles, and finally the analysis, scientific research is always associated with a degree of inherent limitations. Therefore, we would like to elaborate on the limitations associated with this study.

First of all, due to constraints in resources related to this research, the study managed to (only) reach 220 respondents. This sample consisted mainly out of males (N = 149) with 69 females and 2 who respondents who identified as 'other'. Second, the vast majority of the sample has completed an academic education (university bachelor, university master, and PhD) while in general the population of The Netherlands is secondary educated. [20] Finally, although the age of respondents varies from 20 till 84, the average age is 32 years old. In our sample, 74.5% consists of individuals who are in the age categories ranging from 18 till 34. Thus, the older age categories are not adequately represented in our sample. Hence, conclusions about age, in our study the affect of the control variable 'age', should be interpreted with caution since it can only be concluded among the age differences in younger age categories.

Second, although the scenarios were carefully designed and validated with a pilot group, the influence of the stated scenario might not be as desired. The level of abstraction in our study could have influenced the thoughts of respondents. Since they do not feel the 'pain' of risking to lose a certain amount of money, perceptions of risk and security might differ from real life situations.

Third, as we concluded from the ANOVA test (see table 3.3), the control effect for experience should be interpreted with caution. Due to the state of the technologies, pattern recognition and fingerprint recognition have, or are, currently finding their way in everyday life. Facial recognition however, is not yet widely implemented or adopted, hence fewer respondents have experience with this technology.

6.4 Future research

As aforementioned, this study limited itself by looking at two biometric recognition technologies and one additional recognition technology (pattern lock). However, due to the potential offered by other biometric modalities [48, 47], future researchers should focus on different biometric recognition technologies, especially if these recognition technologies continue to improve and meet required standards. Doing so will help creating a more comprehensive understanding of the differences between, and perhaps preferences for certain technologies.

Second, as the sample forms a limitation for this study, future researchers could conduct a larger scale study with a more representative sample, that is a sample that better reflects the demographic composition of The Netherlands (or any country in which the study is performed) regarding the distribution of age, gender and education level. Doing so will result in stronger evidence for conclusions which might validate or counterclaim our findings.

Third, as a consequence of our methodology, the nature of this study could be perceived as abstract. In case respondents had no experience using the technology, we relied on their imagination. To validate our results a less abstract research method should be applied. For example, studies could apply an experimental setting in which a group of participants had to perform the activities in real life. Truly interacting and experiencing the different technologies in the described setting could indicate different perceptions.

Fourth, since some variables of both face and pattern recognition significantly varied from fingerprint recognition regarding Behavioral Intention, but not all scenarios, it would be interesting to include more variables in addition to our proposed model. Doing so might result in a more comprehensive understanding of factors that account for these variations.

Bibliography

[1] Mohamad El-Abed, Christophe Charrier, and Christophe Rosenberger. "Evaluation of biometric systems". In: *New Trends and developments in biometrics.* InTech, 2012.

[2] Mohamad El-Abed et al. "A study of users' acceptance and satisfaction of biometric systems". In: *Security Technology (ICCST), 2010 IEEE International Carnahan Conference on.* ieee. 2010, pp. 170–178.

[3] *About Face ID advanced technology.* Oct. 2018. URL: `https://support.apple.com/en-us/HT208108`.

[4] Olufemi Sunday Adeoye. "A survey of emerging biometric technologies". In: *International Journal of Computer Applications* 10 (2010).

[5] Ritu Agarwal and Jayesh Prasad. "A conceptual and operational definition of personal innovativeness in the domain of information technology". In: *Information systems research* 9.2 (1998), pp. 204–215.

[6] Ritu Agarwal et al. "Early and late adopters of IT innovations: extensions to innovation diffusion theory". In: *Proceedings of the DIGIT Conference.* 1998, pp. 1–18.

[7] Icek Ajzen. "From intentions to actions: A theory of planned behavior". In: *Action control.* Springer, 1985, pp. 11–39.

[8] Icek Ajzen. "The theory of planned behavior". In: *Organizational behavior and human decision processes* 50.2 (1991), pp. 179–211.

[9] Icek Ajzen and Martin Fishbein. "The prediction of behavioral intentions in a choice situation". In: *Journal of experimental social psychology* 5.4 (1969), pp. 400–416.

[10] Icek Ajzen and Martin Fishbein. "Understanding attitudes and predicting social behaviour". In: (1980).

[11] Ulun Akturan and Nuray Tezcan. "Mobile banking adoption of the youth market: Perceptions and intentions". In: *Marketing Intelligence & Planning* 30.4 (2012), pp. 444–459.

[12] Adam J Aviv et al. "Smudge Attacks on Smartphone Touch Screens." In: *Woot* 10 (2010), pp. 1–7.

[13] Stuart J Barnes and Brian Corbitt. "Mobile banking: concept and potential". In: *International Journal of Mobile Communications* 1.3 (2003), pp. 273–288.

[14] Reuben M Baron and David A Kenny. “The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations.” In: *Journal of personality and social psychology* 51.6 (1986), p. 1173.

[15] Cyrille Bataller, Alastair Partington, and Shemsi LHassani. *Biometric Modalities Guidelines.* PowerPoint Presentation. 2013.

[16] Gazal Betab and Ranjeet Kaur Sandhu. “Fingerprints in Automated Teller Machine-A Survey”. In: *International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249* 8958 (2014).

[17] Maatschappelijk Overleg Betalingsverkeer. *Biometrics in payment systems.* Maatschappelijk Overleg Betalingsverkeer, May 11, 2017.

[18] Robert Biddle, Sonia Chiasson, and Paul C Van Oorschot. “Graphical passwords: Learning from the first twelve years”. In: *ACM Computing Surveys (CSUR)* 44.4 (2012), p. 19.

[19] Joseph Bradley. “If we build it they will come? The technology acceptance model”. In: *Information systems theory.* Springer, 2012, pp. 19–36.

[20] CBS. *Cijfers - Onderwijs.* 2018. URL: `https://longreads.cbs.nl/trends18/maatschappij/cijfers/onderwijs/` (visited on 10/25/2018).

[21] Jiajun Jim Chen and Carl Adams. “User acceptance of mobile payments: a theoretical model for mobile payments”. In: *Proceedings of the Fifth International Conference on Electronic Business (ICEB), Hong Kong.* 2005.

[22] Lei-Da Chen. “A theoretical model of consumer acceptance of mpayment”. In: *AMCIS 2006 Proceedings* (2006), p. 247.

[23] National Research Council, Whither Biometrics Committee, et al. *Biometric recognition: challenges and opportunities.* National Academies Press, 2010.

[24] James M Curran and Matthew L Meuter. “Self-service technology adoption: comparing three technologies”. In: *Journal of services marketing* 19.2 (2005), pp. 103–113.

[25] Tomi Dahlberg, Jie Guo, and Jan Ondrus. “A critical review of mobile payment research”. In: *Electronic Commerce Research and Applications* 14.5 (2015), pp. 265–284.

[26] Fred D Davis. “A technology acceptance model for empirically testing new end-user information systems: Theory and results”. PhD thesis. Massachusetts Institute of Technology, 1985.

[27] Fred D Davis. “Perceived usefulness, perceived ease of use, and user acceptance of information technology”. In: *MIS quarterly* (1989), pp. 319–340.

[28] Fred D Davis, Richard P Bagozzi, and Paul R Warshaw. “User acceptance of computer technology: a comparison of two theoretical models”. In: *Management science* 35.8 (1989), pp. 982–1003.

[29] Gwarlann De Kerviler, Nathalie TM Demoulin, and Pietro Zidda. “Adoption of in-store mobile payment: Are perceived risk and convenience the only drivers?” In: *Journal of Retailing and Consumer Services* 31 (2016), pp. 334–344.

[30] Mary Dr Lowth. *Health Information - Episcleritis and Scleritis*. 2015. URL: http://www.hershamsurgery.nhs.uk/the-practice/health-information/?arturi=aHR0cDovL2FwaS5wYXRpZW50LmNvLnVrL2NvbnRlbnQvcGlsL2VwaXNjbGVyaXRpcy1hbm 5C%2FYXBpa2V5PTFkN2I4NWVhLTAyMWYtNDEyM2FiNTA%5C%3D (visited on 07/09/2018).

[31] Wafa Elgarah and Natalia Falaleeva. "Adoption of biometric technology: Information privacy in TAM". In: *AMCIS 2005 Proceedings* (2005), p. 222.

[32] Martin Fishbein and Icek Ajzen. *Belief, attitude, intention and behavior: An introduction to theory and research*. 1975.

[33] Claes Fornell and David F Larcker. "Structural equation models with unobservable variables and measurement error: Algebra and statistics". In: *Journal of marketing research* (1981), pp. 382–388.

[34] David Gefen, Elena Karahanna, and Detmar W Straub. "Inexperience and experience with online stores: The importance of TAM and trust". In: *IEEE Transactions on engineering management* 50.3 (2003), pp. 307–321.

[35] Berk Gökberk et al. "3D face recognition". In: *Guide to Biometric Reference Systems and Performance Evaluation*. Springer, 2009, pp. 263–295.

[36] Berk Gökberk et al. "3D face recognition: technology and applications". In: *Handbook of Remote Biometrics*. Springer, 2009, pp. 217–246.

[37] John T Gourville. "Eager sellers & stony buyers". In: *Harvard Business Review* 84.6 (2006), pp. 98–106.

[38] Gerik Alexander von Graevenitz. "Biometric authentication in relation to payment systems and ATMs". In: *Datenschutz und Datensicherheit-DuD* 31.9 (2007), pp. 681–683.

[39] Marian Harbach, Alexander De Luca, and Serge Egelman. "The anatomy of smartphone unlocking: A field study of android lock screens". In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM. 2016, pp. 4806–4817.

[40] Alan R Hevner. "A three cycle view of design science research". In: *Scandinavian journal of information systems* 19.2 (2007), p. 4.

[41] Hartmut Hoehle, Eusebio Scornavacca, and Sid Huff. "Three decades of research on consumer adoption and utilization of electronic banking channels: A literature analysis". In: *Decision Support Systems* 54.1 (2012), pp. 122–132.

[42] Kristin Houser. *China can now identify a citizen based on their walk*. Nov. 2018. URL: https://futurism.com/the-byte/gait-recognition-china-surveillance.

[43] Hylke Huys. "Consumer Acceptance of Identification Technology". PhD thesis. Ghent University, 2014.

[44] National Technical Authority for Information Assurance. *Biometrics Guide for Access Control Applications*. Report. Centre for Protection of National Infrastructure, 2008.

[45] Acuity Market Intelligence. *Market Research - Biometric Smartphone Model List*. 2016. URL: http://www.acuity-mi.com/BSP.php (visited on 04/24/2018).

[46] John M Irvine et al. “eigenPulse: Robust human identification from cardiovascular function”. In: *Pattern Recognition* 41.11 (2008), pp. 3427–3435.

[47] Anil K Jain, Ruud Bolle, and Sharath Pankanti. *Biometrics: personal identification in networked society.* Vol. 479. Springer Science & Business Media, 2006.

[48] Anil K Jain and Karthik Nandakumar. “Biometric Authentication: System Security and User Privacy.” In: *IEEE Computer* 45.11 (2012), pp. 87–92.

[49] Anil K Jain, Karthik Nandakumar, and Arun Ross. “50 years of biometric research: Accomplishments, challenges, and opportunities”. In: *Pattern Recognition Letters* 79 (2016), pp. 80–105.

[50] Anil K Jain, Arun A Ross, and Karthik Nandakumar. “Introduction”. In: *Introduction to Biometrics.* Springer, 2011, pp. 1–49.

[51] Anil K Jain, Arun Ross, and Sharath Pankanti. “Biometrics: a tool for information security”. In: *IEEE transactions on information forensics and security* 1.2 (2006), pp. 125–143.

[52] Anil K Jain, Arun Ross, and Salil Prabhakar. “An introduction to biometric recognition”. In: *IEEE Transactions on circuits and systems for video technology* 14.1 (2004), pp. 4–20.

[53] Alice M Johnson. “The technology acceptance model and the decision to invest in information security”. In: *Southern Association of Information Systems Conference.* 2005, pp. 114–118.

[54] Vess L Johnson et al. “Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-Payment services”. In: *Computers in Human Behavior* 79 (2018), pp. 111–122.

[55] Daniel Kahneman and Patrick Egan. *Thinking, fast and slow.* Vol. 1. Farrar, Straus and Giroux New York, 2011.

[56] Ankit Kesharwani and Shailendra Singh Bisht. “The impact of trust and perceived risk on internet banking adoption in India: An extension of technology acceptance model”. In: *International Journal of Bank Marketing* 30.4 (2012), pp. 303–322.

[57] Wael Khalifa, Mohamed I Roushdy, and Abdel-Badeeh M Salem. “A Rough Set Approach for User Identification Based on EEG Signals”. In: *Egyptian Computer Science Journal* 38.3 (2014).

[58] Dan J Kim, Donald L Ferrin, and H Raghav Rao. “A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents”. In: *Decision support systems* 44.2 (2008), pp. 544–564.

[59] Nicole Koenig-Lewis, Adrian Palmer, and Alexander Moll. “Predicting young consumers’ take up of mobile banking services”. In: *International journal of bank marketing* 28.5 (2010), pp. 410–432.

[60] Pekka Laukkanen, Suvi Sinkkonen, and Tommi Laukkanen. “Consumer resistance to internet banking: postponers, opponents and rejectors”. In: *International journal of bank marketing* 26.6 (2008), pp. 440–455.

[61] Tommi Laukkanen and Vesa Kiviniemi. “The role of information in mobile banking resistance”. In: *International Journal of Bank Marketing* 28.5 (2010), pp. 372–388.

[62] Jung-Eun Lee, Anil K Jain, and Rong Jin. “Scars, marks and tattoos (SMT): Soft biometric for suspect and victim identification”. In: *Biometrics Symposium, 2008. BSYM’08.* IEEE. 2008, pp. 1–8.

[63] Ming-Chi Lee. “Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit”. In: *Electronic commerce research and applications* 8.3 (2009), pp. 130–141.

[64] Hongxiu Li, Yong Liu, and Jukka Heikkilä. “Understanding the Factors Driving NFC-Enabled Mobile Payment Adoption: an Empirical Investigation.” In: *PACIS.* 2014, p. 231.

[65] Francisco Liébana-Cabanillas, Francisco Muñoz-Leiva, and Juan Sánchez-Fernández. “A global approach to the analysis of user behavior in mobile payment systems in the new electronic environment”. In: *Service Business* 12.1 (2018), pp. 25–64.

[66] Rensis Likert. “A technique for the measurement of attitudes.” In: *Archives of psychology* (1932).

[67] Richard G Lomax and Randall E Schumacker. *A beginner’s guide to structural equation modeling.* psychology press, 2004.

[68] Yaobin Lu et al. “Dynamics between the trust transfer process and intention to use mobile payment services: A cross-environment perspective”. In: *Information & Management* 48.8 (2011), pp. 393–403.

[69] Nathan Malkin et al. “The anatomy of smartphone unlocking: Why and how android users around the world lock their phones”. In: *GetMobile: Mobile Computing and Communications* 20.3 (2017), pp. 42–46.

[70] Saunders Mark, Lewis Philip, and Thornhill Adrian. *Research methods for business students.* 2009.

[71] Carolina Martins, Tiago Oliveira, and Aleš Popovič. “Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application”. In: *International Journal of Information Management* 34.1 (2014), pp. 1–13.

[72] Caroline Lancelot Miltgen, Aleš Popovič, and Tiago Oliveira. “Determinants of end-user acceptance of biometrics: Integrating the “Big 3” of technology acceptance with privacy context”. In: *Decision Support Systems* 56 (2013), pp. 103–114.

[73] Gary C Moore and Izak Benbasat. “Development of an instrument to measure the perceptions of adopting an information technology innovation”. In: *Information systems research* 2.3 (1991), pp. 192–222.

[74] Emilio Mordini and Dimitros Tzovaras. *Second generation biometrics: The ethical, legal and social context.* Vol. 11. Springer Science & Business Media, 2012.

[75] Alex Nasonov. “What’s the future for biometrics in global payments?” In: *Biometric Technology Today* 2017.8 (2017), pp. 5–7.

[76] Obi Ogbanufe and Dan J Kim. “Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment”. In: *Decision Support Systems* (2017).

[77] Tiago Oliveira et al. “Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology”. In: *Computers in Human Behavior* 61 (2016), pp. 404–414.

[78] Ananthanarayanan Parasuraman. “Technology Readiness Index (TRI) a multiple-item scale to measure readiness to embrace new technologies”. In: *Journal of service research* 2.4 (2000), pp. 307–320.

[79] Unsang Park, Arun Ross, and Anil K Jain. “Periocular biometrics in the visible spectrum: A feasibility study”. In: *Biometrics: Theory, Applications, and Systems, 2009. BTAS’09. IEEE 3rd International Conference on.* IEEE. 2009, pp. 1–6.

[80] Silvia Parusheva. “A comparative study on the application of biometric technologies for authentication in online banking”. In: *Egyptian Computer Science Journal* 39.4 (2015), pp. 116–127.

[81] Thanh-Thao T Pham and Jonathan C Ho. “The effects of product-related, personal-related factors and attractiveness of alternatives on consumer adoption of NFC-based mobile payments”. In: *Technology in Society* 43 (2015), pp. 159–172.

[82] Philip M Podsakoff et al. “Common method biases in behavioral research: A critical review of the literature and recommended remedies.” In: *Journal of applied psychology* 88.5 (2003), p. 879.

[83] National Biometric Security Project. *Biometric Technology Application Manual Volume 1: Biometric basics.* Vol. 1. National Biometric Security Project, 2008.

[84] National Biometric Security Project. *Biometric Technology Application Manual Volume One: Biometric Basics.* National Biometric Security Project, 2008.

[85] Everett M Rogers. *Diffusion of Innovations.* The Free Press, 1983.

[86] Maria Saaksjarvi. “Consumer adoption of technological innovations”. In: *European Journal of Innovation Management* 6.2 (2003), pp. 90–100.

[87] Hataichanok Saevanee et al. “Continuous user authentication using multimodal biometrics”. In: *Computers & Security* 53 (2015), pp. 234–246.

[88] Paul Gerhardt Schierz, Oliver Schilke, and Bernd W Wirtz. “Understanding consumer acceptance of mobile payment services: An empirical analysis”. In: *Electronic commerce research and applications* 9.3 (2010), pp. 209–216.

[89] Murray Scott, Thomas Acton, and Martin Hughes. “An assessment of biometric identities as a standard for e-government services”. In: *International Journal of Services and Standards* 1.3 (2004), pp. 271–286.

[90] NEDAP Security. *Selecting the appropriate biometric technology.* Report. NEDAP, 2018.

[91] Aijaz A Shaikh and Heikki Karjaluoto. “Mobile banking adoption: A literature review”. In: *Telematics and Informatics* 32.1 (2015), pp. 129–142.

[92] Siraj A Shaikh and Joseph R Rabaiotti. “Characteristic trade-offs in designing large-scale biometric-based identity management systems”. In: *Journal of Network and Computer Applications* 33.3 (2010), pp. 342–351.

[93] Rana Tassabehji and Mumtaz A Kamala. “Improving e-banking security with biometrics: modelling user attitudes and acceptance”. In: *New Technologies, Mobility and Security (NTMS), 2009 3rd International Conference on.* IEEE. 2009, pp. 1–6.

[94] Rakhi Thakur and Mala Srivastava. “Adoption readiness, personal innovativeness, perceived risk and usage intention across customer groups for mobile payment services in India”. In: *Internet Research* 24.3 (2014), pp. 369–392.

[95] James YL Thong, Se-Joon Hong, and Kar Yan Tam. “The effects of post-adoption beliefs on the expectation-confirmation model for information technology continuance”. In: *International Journal of Human-Computer Studies* 64.9 (2006), pp. 799–810.

[96] KP Tripathi. “A comparative study of biometric technologies with reference to human interface”. In: *International Journal of Computer Applications* 14.5 (2011), pp. 10–15.

[97] JA Unar, Woo Chaw Seng, and Almas Abbasi. “A review of biometric technology along with trends and prospects”. In: *Pattern recognition* 47.8 (2014), pp. 2673–2688.

[98] Hans Van der Heijden. “User acceptance of hedonic information systems”. In: *MIS quarterly* (2004), pp. 695–704.

[99] Robert E Vanaman. *Biometric Facial Recognition Database Systems.* 2014. URL: `https://eforensicsmag.com/biometric-facial-recognition-database-systems/` (visited on 05/07/2018).

[100] Raymond Nicolaas Johan Veldhuis. *Biometrie-op de grens tussen techniek en mens.* University of Twente, 2014.

[101] Viswanath Venkatesh, James YL Thong, and Xin Xu. “Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology”. In: *MIS quarterly* (2012), pp. 157–178.

[102] Viswanath Venkatesh et al. “User acceptance of information technology: Toward a unified view”. In: *MIS quarterly* (2003), pp. 425–478.

[103] Sitalakshmi Venkatraman and Indika Delpachitra. “Biometrics in banking security: a case study”. In: *Information Management & Computer Security* 16.4 (2008), pp. 415–430.

[104] Emanuel Von Zezschwitz et al. “Easy to draw, but hard to trace?: On the observability of grid-based (un) lock patterns”. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems.* ACM. 2015, pp. 2339–2342.

[105] J Walker and S Maddan. “Factor analysis, path analysis, and structural equation modeling”. In: *Statistics in Criminology and Criminal Justice: Analysis and Interpretation, 3rd edn. USA: Jones & Bartlett Publishers* (2008), pp. 325–51.

[106] Lisa Wessels and Judy Drennan. “An investigation of consumer acceptance of M-banking”. In: *International Journal of bank marketing* 28.7 (2010), pp. 547–568.

[107] Heng Xu and Sumeet Gupta. “The effects of privacy concerns and personal innovativeness on potential and experienced customers’ adoption of location-based services”. In: *Electronic Markets* 19.2-3 (2009), pp. 137–149.

[108] Shuiqing Yang et al. “Mobile payment services adoption across time: An empirical study of the effects of behavioral beliefs, social influences, and personal traits”. In: *Computers in Human Behavior* 28.1 (2012), pp. 129–142.

Chapter 7

Appendices

7.1 Appendix A

This appendix discusses the different scenarios which are provided to the respondents in a randomized manner. Starting on the next page, every scenario will be described in both English and Dutch.

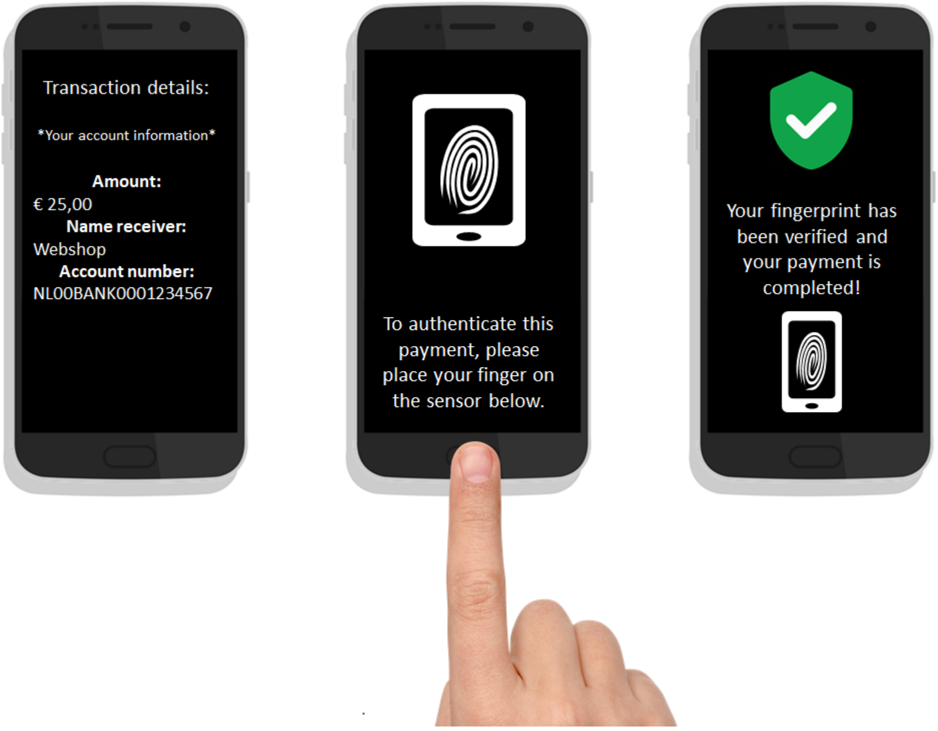
7.1.1 Scenario 1: Fingerprint recognition - Low value

Imagine yourself being in the following situation:

Your bank offers the possibility to confirm (authenticate) payments using a **fingerprint.** After reading the message regarding this technology you decide to give it a try, thus after completing the configuration, it is now possible to **confirm payments using your fingerprint(s).**

Some days after the configuration, you want to place an order at an online webshop for a price of **25 euro**s and you want to pay online (e.g. using iDeal). After choosing your bank at the check-out, your mobile banking app on your smartphone or tablet shows a notification. After opening this app, you discover it asks you to confirm the payment of **25 euros.** After checking the details of the order and the total amount, you want to confirm your payment. Since you have enabled fingerprint-authentication you place one of your scanned fingerprints on the sensor of your mobile device (a smartphone or tablet). Immediately after placing your finger on the sensor, the device recognizes the fingerprint and the payment is confirmed and the total amount due will be deducted from the bank account.

Keep this scenario in mind while answering the following questions.



Transaction details:

Your account information

Amount:
€ 25,00
Name receiver:
Webshop
Account number:
NL00BANK0001234567

To authenticate this payment, please place your finger on the sensor below.

Your fingerprint has been verified and your payment is completed!

Figure 7.1: Scenario 1 English

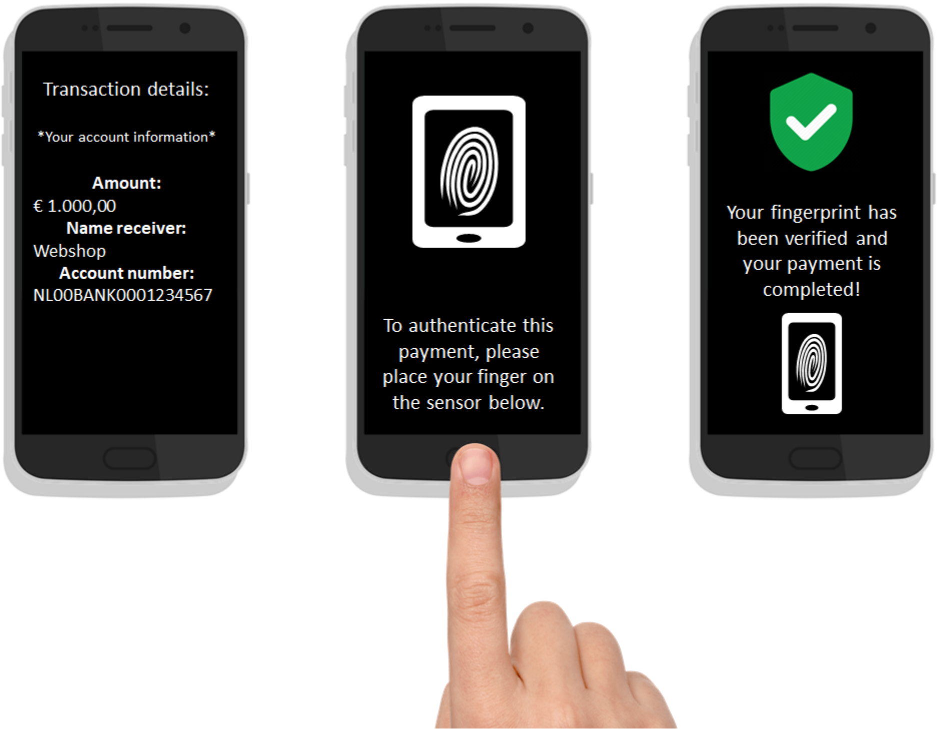
7.1.2 Scenario 2: Fingerprint recognition - High value

Imagine yourself being in the following situation:

Your bank offers the possibility to confirm (authenticate) payments using a **fingerprint.** After reading the message regarding this technology you decide to give it a try, thus after completing the configuration, it is now possible to **confirm payments using your fingerprint(s).**

Some days after the configuration, you want to place an order at an online webshop for a price of **1.000 (thousand) euros** and you want to pay online (e.g. using iDeal). After choosing your bank at the check-out, your mobile banking app on your smartphone or tablet shows a notification. After opening this app, you discover it asks you to confirm the payment of **1.000 (thousand) euros.** After checking the details of the order and the total amount, you want to confirm your payment. Since you have enabled fingerprint-authentication you place one of your scanned fingerprints on the sensor of your mobile device (a smartphone or tablet). Immediately after placing your finger on the sensor, the device recognizes the fingerprint and the payment is confirmed and the total amount due will be deducted from the bank account.

Keep this scenario in mind while answering the following questions.



Transaction details:

Your account information

Amount:
€ 1.000,00
Name receiver:
Webshop
Account number:
NL00BANK0001234567

To authenticate this payment, please place your finger on the sensor below.

Your fingerprint has been verified and your payment is completed!

Figure 7.2: Scenario 2 English

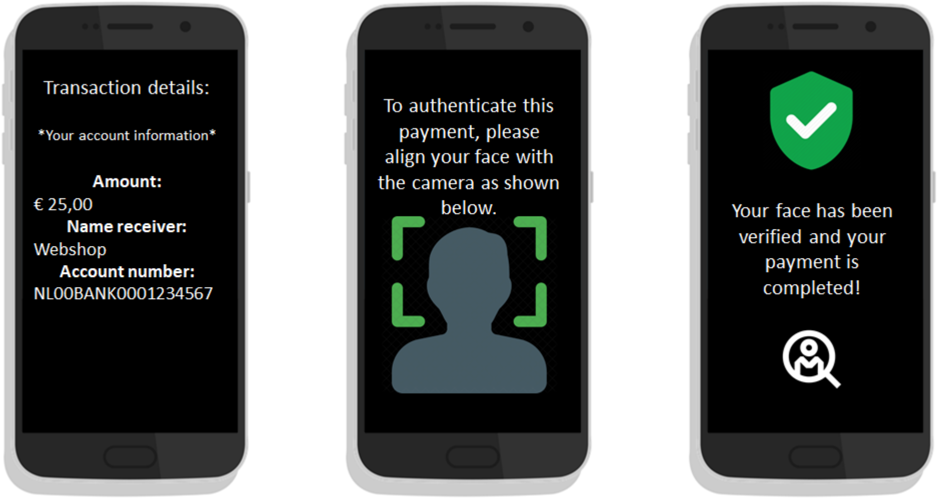
7.1.3 Scenario 3: Facial recognition - Low value

Imagine yourself being in the following situation:

Your bank offers the possibility to confirm (authenticate) payments using **facial recognition.** After reading the message regarding this technology you decide to give it a try, thus after completing the configuration, it is now possible to **confirm payments using facial recognition.**

Some days after the configuration, you want to place an order at an online webshop for a price of 25 euros and you want to pay online (e.g. using iDeal). After choosing your bank at the check-out, your mobile banking app on your smartphone or tablet shows a notification. After opening this app, you discover it asks you to confirm the payment of 25 euros. After checking the details of your order and the total amount, you want to confirm your payment. Since you have enabled facial recognition, you hold your mobile device (smartphone or tablet) in front of you. Almost immediately the camera recognizes your face. You have now confirmed the payment and the total amount due will be deducted from the bank account.

Keep this scenario in mind while answering the following questions.



Transaction details:

Your account information

Amount:
€ 25,00
Name receiver:
Webshop
Account number:
NL00BANK0001234567

To authenticate this payment, please align your face with the camera as shown below.

Your face has been verified and your payment is completed!

Figure 7.3: Scenario 3 English

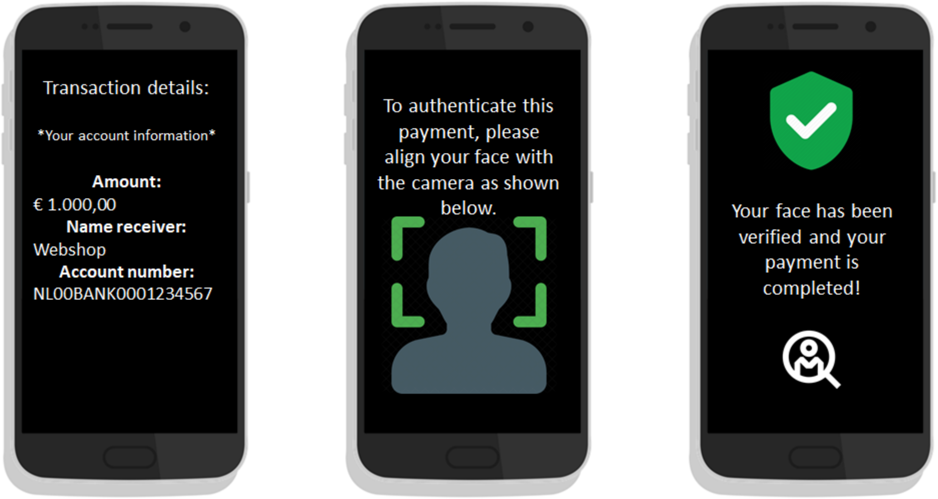
7.1.4 Scenario 4: Facial recognition - High value

Imagine yourself being in the following situation:

Your bank offers the possibility to confirm (authenticate) payments using **facial recognition.** After reading the message regarding this technology you decide to give it a try, thus after completing the configuration, it is now possible to **confirm payments using facial recognition.**

Some days after the configuration, you want to place an order at an online webshop for a price of 1.000 (thousand) euros and you want to pay online (e.g. using iDeal). After choosing your bank at the check-out, your mobile banking app on your smartphone or tablet shows a notification. After opening this app, you discover it asks you to confirm the payment of 1.000 (thousand) euros. After checking the details of your order and the total amount, you want to confirm your payment. Since you have enabled facial recognition, you hold your mobile device (smartphone or tablet) in front of you. Almost immediately the camera recognizes your face. You have now confirmed the payment and the total amount due will be deducted from the bank account.

Keep this scenario in mind while answering the following questions.



Transaction details:

Your account information

Amount:
€ 1.000,00
Name receiver:
Webshop
Account number:
NL00BANK0001234567

To authenticate this payment, please align your face with the camera as shown below.

Your face has been verified and your payment is completed!

Figure 7.4: Scenario 4 English

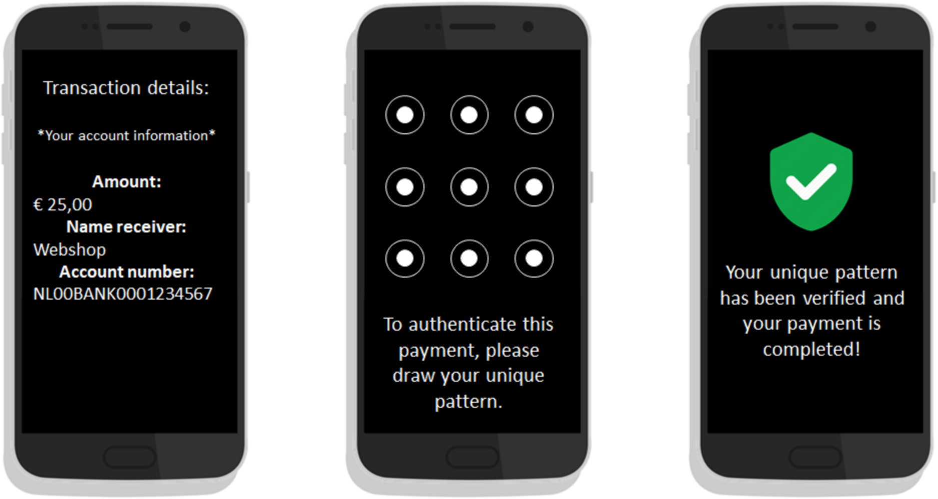
7.1.5 Scenario 5: Pattern recognition - Low value

Imagine yourself being in the following situation:

Your bank offers the possibility to confirm (authenticate) payments using **pattern recognition.** After reading the message regarding this technology you decide to give it a try, thus after completing the configuration, it is now possible to **confirm payments by drawing a pattern using your fingers.**

Some days after the configuration, you want to place an order at an online webshop for a price of 25 euros and you want to pay online (e.g. using iDeal). After choosing your bank at the check-out, your mobile banking app on your smartphone or tablet shows a notification. After opening this app, you discover it asks you to confirm the payment of 25 euros. After checking the details of your order and the total amount, you want to confirm your payment. Since you have enabled pattern recognition, you draw your pattern using your finger on your mobile device (smartphone or tablet). Almost immediately after completion, the device recognizes your pattern. You have now confirmed the payment and the total amount due will be deducted from the bank account.

Keep this scenario in mind while answering the following questions.



Transaction details:

Your account information

Amount:
€ 25,00
Name receiver:
Webshop
Account number:
NL00BANK0001234567

To authenticate this payment, please draw your unique pattern.

Your unique pattern has been verified and your payment is completed!

Figure 7.5: Scenario 5 English

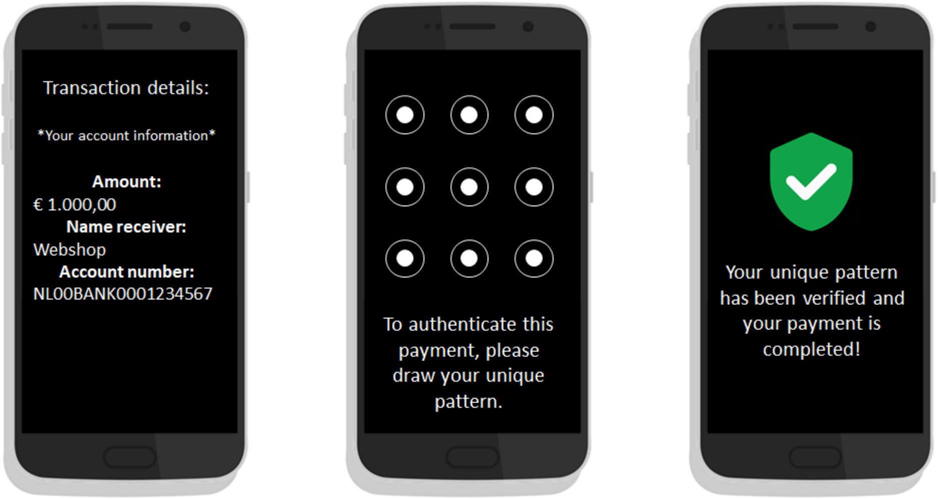
7.1.6 Scenario 6: Pattern recognition - High value

Imagine yourself being in the following situation:

Your bank offers the possibility to confirm (authenticate) payments using **pattern recognition.** After reading the message regarding this technology you decide to give it a try, thus after completing the configuration, it is now possible to **confirm payments by drawing a pattern using your fingers.**

Some days after the configuration, you want to place an order at an online webshop for a price of 1.000 (thousand) euros and you want to pay online (e.g. using iDeal). After choosing your bank at the check-out, your mobile banking app on your smartphone or tablet shows a notification. After opening this app, you discover it asks you to confirm the payment of 1.000 (thousand) euros. After checking the details of your order and the total amount, you want to confirm your payment. Since you have enabled pattern recognition, you draw your pattern using your finger on your mobile device (smartphone or tablet). Almost immediately after completion, the device recognizes your pattern. You have now confirmed the payment and the total amount due will be deducted from the bank account.

Keep this scenario in mind while answering the following questions.



Transaction details:

Your account information

Amount:
€ 1.000,00
Name receiver:
Webshop
Account number:
NL00BANK0001234567

To authenticate this payment, please draw your unique pattern.

Your unique pattern has been verified and your payment is completed!

Figure 7.6: Scenario 6 English

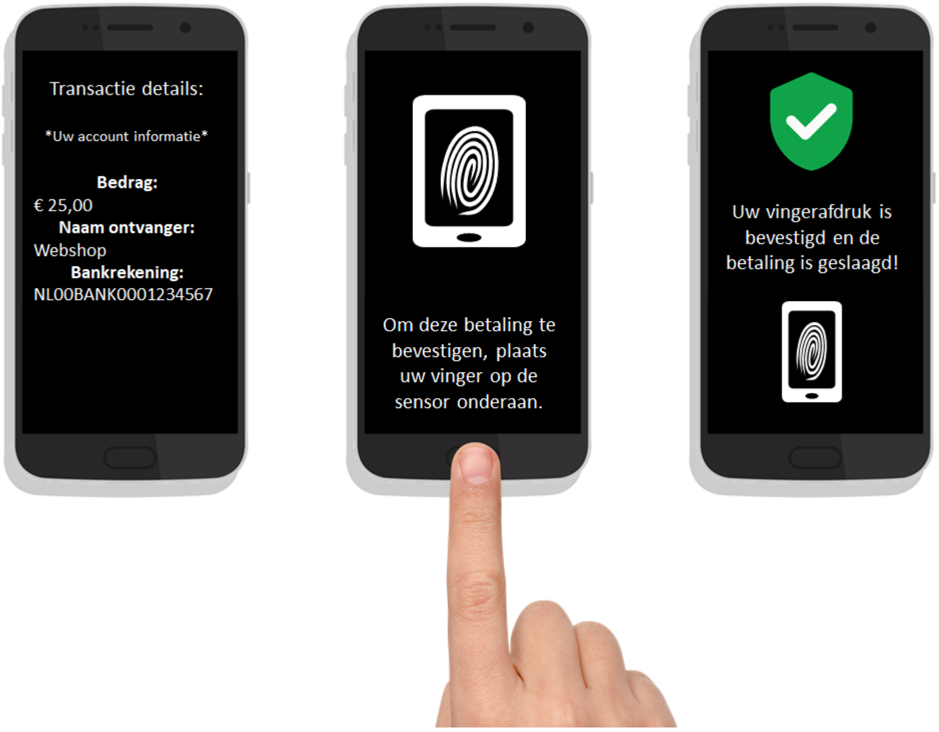
7.1.7 Scenario 1: Vingerafdrukherkenning - Laag bedrag

Stelt u zich voor dat zich in de volgende situatie bevindt:

Uw bank biedt de mogelijkheid om voortaan betalingen te bevestigen (authentiseren) middels een **vingerafdruk**. Na het zien van dit bericht besluit u om dit te proberen, ofwel na het instellen hiervan is het voortaan mogelijk om **middels vingerafdruk(ken) betalingen te bevestigen.**

Enkele dagen nadat u dit heeft ingesteld, wilt u een bestelling plaatsen bij een (online) webshop waarbij het een bedrag van **25 euro** betreft. U wilt dit online betalen (bijv. door gebruik te maken van iDeal). Nadat u bij de kassa uw bank heeft gekozen, ontvangt u een notificatie van uw mobiel bankieren app van uw smartphone of tablet. U opent de melding en komt erachter dat deze vraagt om de betaling van **25 euro** te controleren. Nadat u de details van de bestelling heeft bekeken evenals het totale aankoopbedrag, wilt u de betaling bevestigen. Aangezien u vingerafdruk herkenning heeft ingesteld, plaatst u één van uw vingers op de sensor van het mobiele apparaat (smartphone of tablet). Vrijwel direct na het plaatsen van uw vinger herkent het apparaat u, is de betaling bevestigd en wordt het verschuldigde bedrag van de rekening afgeschreven.

Houdt dit scenario in gedachten bij het beantwoorden van de volgende vragen.



Transactie details:

Uw account informatie

Bedrag:
€ 25,00
Naam ontvanger:
Webshop
Bankrekening:
NL00BANK0001234567

Om deze betaling te bevestigen, plaats uw vinger op de sensor onderaan.

Uw vingerafdruk is bevestigd en de betaling is geslaagd!

Figure 7.7: Scenario 1 Nederlands

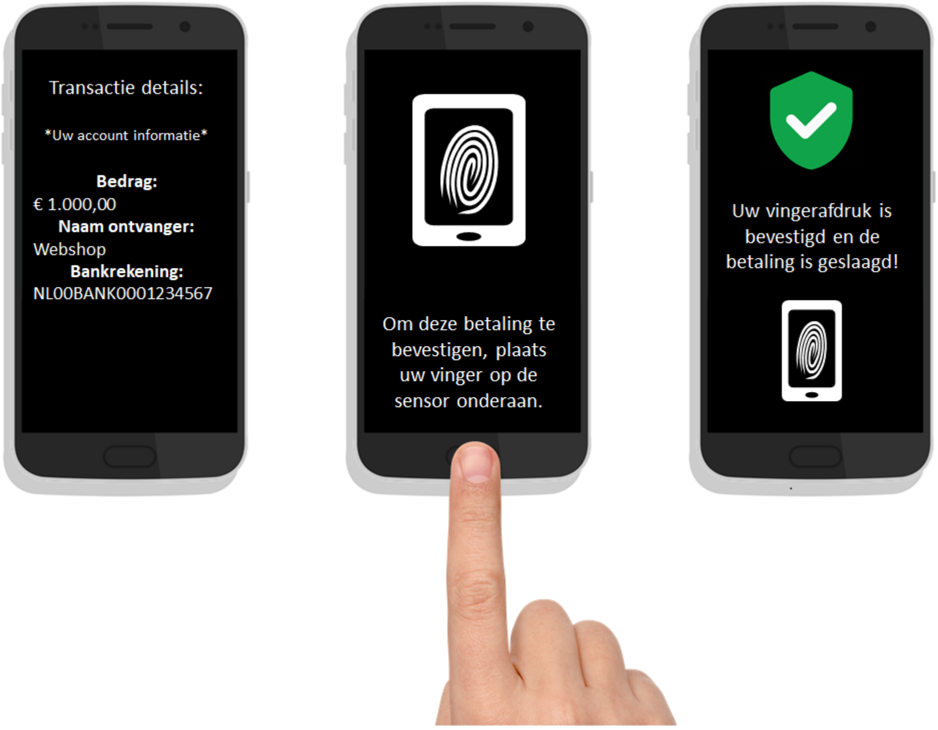
7.1.8 Scenario 2: Vingerafdrukherkenning - Hoog bedrag

Stelt u zich voor dat zich in de volgende situatie bevindt:

Uw bank biedt de mogelijkheid om voortaan betalingen te bevestigen (authentiseren) middels een **vingerafdruk**. Na het zien van dit bericht besluit u om dit te proberen, ofwel na het instellen hiervan is het voortaan mogelijk om **middels vingerafdruk(ken) betalingen te bevestigen.**

Enkele dagen nadat u dit heeft ingesteld, wilt u een bestelling plaatsen bij een (online) webshop waarbij het een bedrag van **1.000 (duizend) euro** betreft. U wilt dit online betalen (bijv. door gebruik te maken van iDeal). Nadat u bij de kassa uw bank heeft gekozen, ontvangt u een notificatie van uw mobiel bankieren app van uw smartphone of tablet. U opent de melding en komt erachter dat deze vraagt om de betaling van **1.000 (duizend) euro** te controleren. Nadat u de details van de bestelling heeft bekeken evenals het totale aankoopbedrag, wilt u de betaling bevestigen. Aangezien u vingerafdruk herkenning heeft ingesteld, plaatst u één van uw vingers op de sensor van het mobiele apparaat (smartphone of tablet). Vrijwel direct na het plaatsen van uw vinger herkent het apparaat u, is de betaling bevestigd en wordt het verschuldigde bedrag van de rekening afgeschreven.

Houdt dit scenario in gedachten bij het beantwoorden van de volgende vragen.



Transactie details:

Uw account informatie

Bedrag:
€ 1.000,00
Naam ontvanger:
Webshop
Bankrekening:
NL00BANK0001234567

Om deze betaling te bevestigen, plaats uw vinger op de sensor onderaan.

Uw vingerafdruk is bevestigd en de betaling is geslaagd!

Figure 7.8: Scenario 2 Nederlands

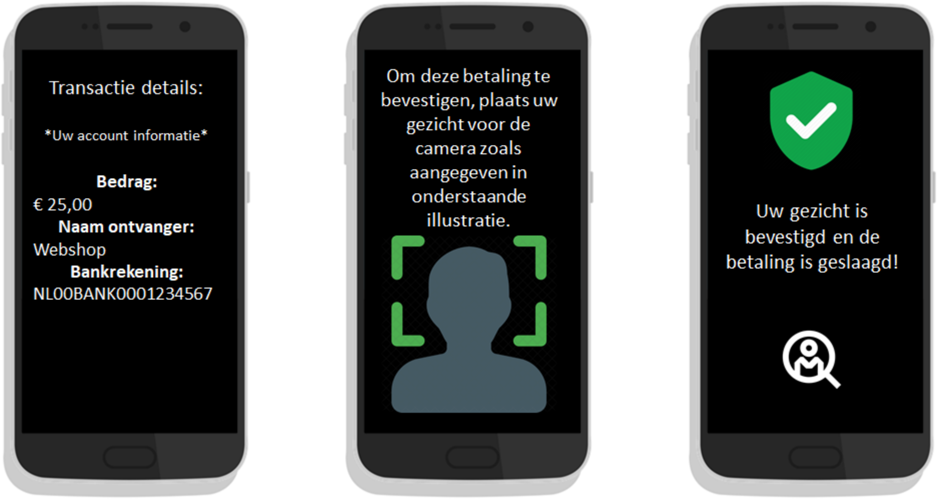
7.1.9 Scenario 3: Gezichtsherkenning - Laag bedrag

Stelt u zich voor dat zich in de volgende situatie bevindt:

Uw bank biedt de mogelijkheid om voortaan betalingen te bevestigen (authentiseren) middels **gezichtsherkenning.** Na het zien van dit bericht besluit u om dit te proberen, ofwel na het instellen hiervan is het voortaan mogelijk om **middels gezichtsherkenning betalingen te bevestigen.**

Enkele dagen nadat u dit heeft ingesteld, wilt u een bestelling plaatsen bij een (online) webshop waarbij het een bedrag van **25 euro** betreft. U wilt dit online betalen (bijv. door gebruik te maken van iDeal). Nadat u bij de kassa uw bank heeft gekozen, ontvangt u een notificatie van uw mobiel bankieren app van uw smartphone of tablet. U opent de melding en komt erachter dat deze vraagt om de betaling van **25 euro** te controleren. Nadat u de details van de bestelling heeft bekeken evenals het totale aankoopbedrag, wilt u de betaling bevestigen. Aangezien u gezichtsherkenning heeft ingesteld, houdt u uw mobiele apparaat (smartphone of tablet) voor uw gezicht en vrijwel direct herkent de camera uw gezicht, is de betaling bevestigd en wordt het verschuldigde bedrag van de rekening afgeschreven.

Houdt dit scenario in gedachten bij het beantwoorden van de volgende vragen.



Transactie details:

Uw account informatie

Bedrag:
€ 25,00
Naam ontvanger:
Webshop
Bankrekening:
NL00BANK0001234567

Om deze betaling te bevestigen, plaats uw gezicht voor de camera zoals aangegeven in onderstaande illustratie.

Uw gezicht is bevestigd en de betaling is geslaagd!

Figure 7.9: Scenario 3 Nederlands

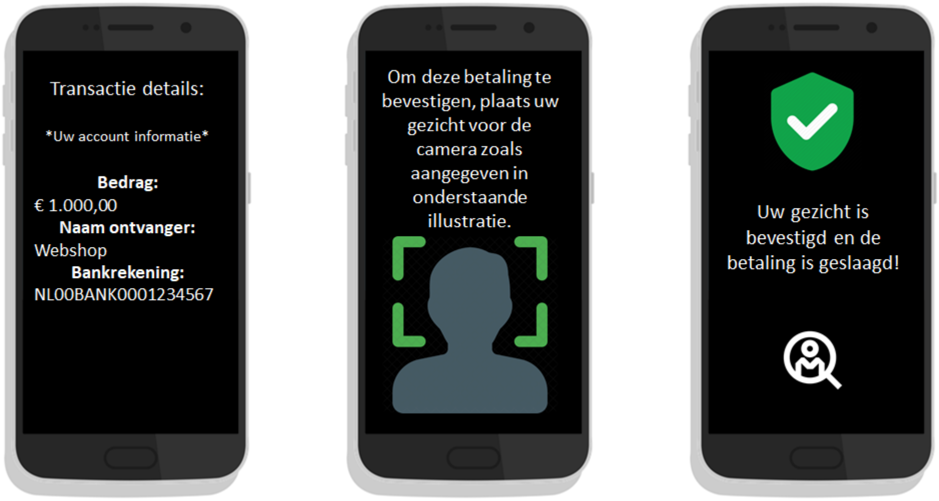
7.1.10 Scenario 4: Gezichtsherkenning - Hoog bedrag

Stelt u zich voor dat zich in de volgende situatie bevindt:

Uw bank biedt de mogelijkheid om voortaan betalingen te bevestigen (authentiseren) middels **gezichtsherkenning.** Na het zien van dit bericht besluit u om dit te proberen, ofwel na het instellen hiervan is het voortaan mogelijk om **middels gezichtsherkenning betalingen te bevestigen.**

Enkele dagen nadat u dit heeft ingesteld, wilt u een bestelling plaatsen bij een (online) webshop waarbij het een bedrag van **1.000 (duizend) euro** betreft. U wilt dit online betalen (bijv. door gebruik te maken van iDeal). Nadat u bij de kassa uw bank heeft gekozen, ontvangt u een notificatie van uw mobiel bankieren app van uw smartphone of tablet. U opent de melding en komt erachter dat deze vraagt om de betaling van **1.000 (duizend) euro** te controleren. Nadat u de details van de bestelling heeft bekeken evenals het totale aankoopbedrag, wilt u de betaling bevestigen. Aangezien u gezichtsherkenning heeft ingesteld, houdt u uw mobiele apparaat (smartphone of tablet) voor uw gezicht en vrijwel direct herkent de camera uw gezicht, is de betaling bevestigd en wordt het verschuldigde bedrag van de rekening afgeschreven.

Houdt dit scenario in gedachten bij het beantwoorden van de volgende vragen.



Transactie details:

Uw account informatie

Bedrag:
€ 1.000,00
Naam ontvanger:
Webshop
Bankrekening:
NL00BANK0001234567

Om deze betaling te bevestigen, plaats uw gezicht voor de camera zoals aangegeven in onderstaande illustratie.

Uw gezicht is bevestigd en de betaling is geslaagd!

Figure 7.10: Scenario 4 Nederlands

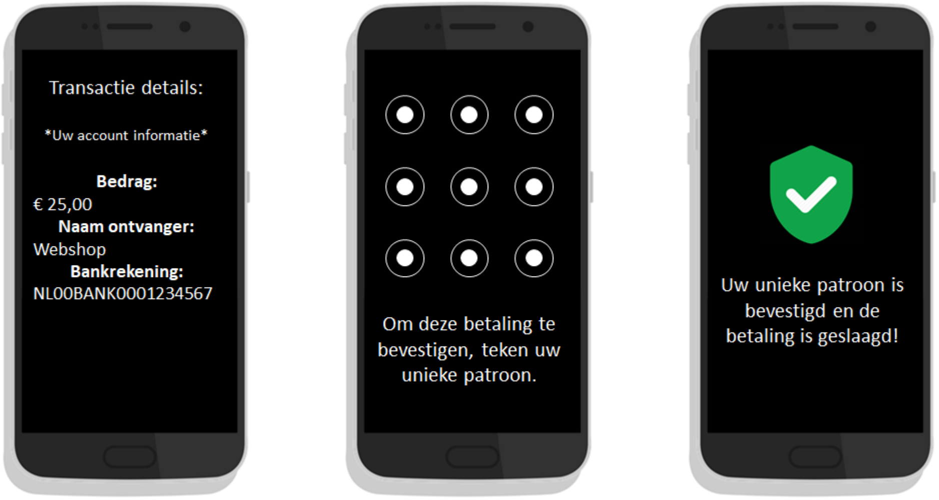
7.1.11 Scenario 5: Patroonherkenning - Laag bedrag

Stelt u zich voor dat zich in de volgende situatie bevindt:

Uw bank biedt de mogelijkheid om voortaan betalingen te bevestigen (authentiseren) middels het tekenen van een zelf ingesteld **patroon op uw mobiele apparaat.** Na het zien van dit bericht besluit u om dit te proberen, ofwel na het instellen hiervan is het voortaan mogelijk om **betalingen te bevestigen door een patroon te tekenen met uw vinger.**

Enkele dagen nadat u dit heeft ingesteld, wilt u een bestelling plaatsen bij een (online) webshop waarbij het een bedrag van **25 euro** betreft. U wilt dit online betalen (bijv. door gebruik te maken van iDeal). Nadat u bij de kassa uw bank heeft gekozen, ontvangt u een notificatie van uw mobiel bankieren app van uw smartphone of tablet. U opent de melding en komt erachter dat deze vraagt om de betaling van **25 euro** te controleren. Nadat u de details van de bestelling heeft bekeken evenals het totale aankoopbedrag, wilt u de betaling bevestigen. Aangezien u patroonherkenning heeft ingesteld, tekent u met uw vinger het ingestelde patroon en vrijwel direct herkent het apparaat uw patroon en is de betaling bevestigd en wordt het verschuldigde bedrag van de rekening afgeschreven.

Houdt dit scenario in gedachten bij het beantwoorden van de volgende vragen.



Transactie details:

Uw account informatie

Bedrag:
€ 25,00
Naam ontvanger:
Webshop
Bankrekening:
NL00BANK0001234567

Om deze betaling te bevestigen, teken uw unieke patroon.

Uw unieke patroon is bevestigd en de betaling is geslaagd!

Figure 7.11: Scenario 5 Nederlands

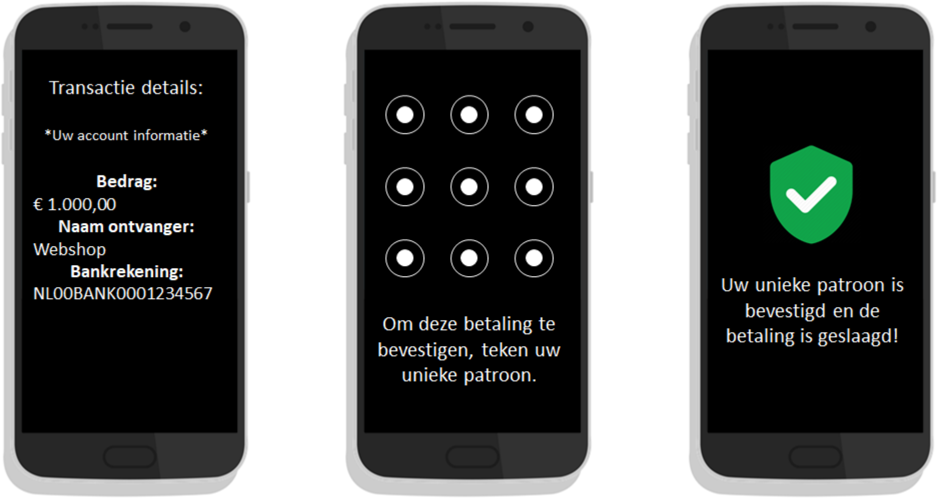
7.1.12 Scenario 6: Patroonherkenning - Hoog bedrag

Stelt u zich voor dat zich in de volgende situatie bevindt:

Uw bank biedt de mogelijkheid om voortaan betalingen te bevestigen (authentiseren) middels het tekenen van een zelf ingesteld **patroon op uw mobiele apparaat.** Na het zien van dit bericht besluit u om dit te proberen, ofwel na het instellen hiervan is het voortaan mogelijk om **betalingen te bevestigen door een patroon te tekenen met uw vinger.**

Enkele dagen nadat u dit heeft ingesteld, wilt u een bestelling plaatsen bij een (online) webshop waarbij het een bedrag van **1.000 (duizend) euro** betreft. U wilt dit online betalen (bijv. door gebruik te maken van iDeal). Nadat u bij de kassa uw bank heeft gekozen, ontvangt u een notificatie van uw mobiel bankieren app van uw smartphone of tablet. U opent de melding en komt erachter dat deze vraagt om de betaling van **1.000 (duizend) euro** te controleren. Nadat u de details van de bestelling heeft bekeken evenals het totale aankoopbedrag, wilt u de betaling bevestigen. Aangezien u patroonherkenning heeft ingesteld, tekent u met uw vinger het ingestelde patroon en vrijwel direct herkent het apparaat uw patroon en is de betaling bevestigd en wordt het verschuldigde bedrag van de rekening afgeschreven.

Houdt dit scenario in gedachten bij het beantwoorden van de volgende vragen.



Transactie details:

Uw account informatie

Bedrag:
€ 1.000,00
Naam ontvanger:
Webshop
Bankrekening:
NL00BANK0001234567

Om deze betaling te bevestigen, teken uw unieke patroon.

Uw unieke patroon is bevestigd en de betaling is geslaagd!

Figure 7.12: Scenario 6 Nederlands

7.2 Appendix B

Construct (Abbr.)	Item	Source
Innovativeness (Innov)	1. When I hear about a new information technology, I would look for ways to experiment with it.	Agarwal et al. (1998)
	2. Among my peers, I am usually the first to try out a new information technology.	
	3. In general, I am hesitant to try out new information technologies.	
	4. I like to experiment with new information technologies.	
Lifestyle Compatibility (LC)	1. I believe that using mobile biometric* to confirm financial transactions will fit my lifestyle.	Chen (2006)
	2. I believe that using mobile biometric to confirm financial transactions is compatible with the way I like to transfer money.	
	3. I believe that using mobile biometric for financial transactions fits well with my current log-in methods.	
	4. I believe that using mobile biometric to confirm financial transactions will be fun.	
	5. I believe that using mobile biometric is suitable for me.	
Perceived Risk (PR)	1. I think using mobile biometric to authenticate myself in order to confirm financial transactions would have a potential risk.	Pham et al. (2015)
	2. I believe information concerning my transactions authorized using my biometric would be known to others.	
	3. I believe that my savings would be in jeopardy if I use mobile biometric to authenticate myself for a transaction.	
	4. I believe that information concerning my transactions authorized using mobile biometric could be tampered with by others.	
Perceived Privacy Concern (PPC)	1. I am concerned about the amount of personal information I will be required to provide when using mobile biometric.	Chen (2006)
	2. I believe that my personal information stored in the databases for mobile biometric will be protected.	
	3. I believe that my personal information stored in the databases for mobile biometric will be accurate.	
	4. I believe that the personal information I provide for mobile biometric will only be used for the purposes I authorize.	
	5. I believe that using biometric to confirm financial transactions will put my privacy at risk.	
Perceived Security (PS)	1. I believe that mobile biometric provides high levels of security.	Tassabehji et al. (2009)
	2. Using mobile biometric will improve the security of bank account access.	
	3. I feel comfortable using mobile biometric to access my bank account on my mobile devices.	
	4. I would feel more comfortable using mobile biometric instead of passwords for mobile banking.	
Perceived Ease of Use (PEoU)	1. Learning to operate mobile biometric to confirm transactions would be easy for me.	Davis (1989)
	2. I believe using mobile biometric to confirm financial transactions will be easy to understand.	
	3. I would find mobile biometric easy to use.	
	4. I believe that it would be easy for me to become skillful at using mobile biometric.	
	5. I believe that when I use mobile biometric the process will be clear and understandable.	
Behavioral Intention (BI)	1. I plan to use mobile biometric to authorize financial transactions in the future.	Venkatesh et al. (2003)
	2. I intend to use mobile biometric to authorize financial transactions in the future.	
	3. I predict I would use mobile biometric to authorize financial transactions in the future.	

* Biometric refers to the specific recognition technology presented to respondents in the corresponding scenario. Thus, based on this scenario the word biometric was transformed to either fingerprint recognition, facial recognition, or pattern recognition.

7.3 Appendix C

7.3.1 Codebook

Construct	**Construct label**	**Item**	**Item label**
Lifestyle Compatibility	LComp_Mean	LC1	Compatibility1
		LC2	Compatibility2
		LC3	Compatibility3
		LC4	Compatibility4
		LC5	Compatibility5
Perceived Risk	PRisk_Mean	PR1	Risk1
		PR2	Risk2
		PR3	Risk3
		PR4	Risk4
Perceived Privacy Concern	PConcern_mean	REC_PPC1	PrivConcern1R
		PPC2	PrivConcern2
		PPC3	PrivConcern3
		PPC4	PrivConcern4
		REC_PPC5	PrivConcern5R
Perceived Security	PSecurity_Mean	PS1	Security1
		PS2	Security2
		PS3	Security3
		PS4	Security4
Perceived Ease of Use	PEase_Mean	PEoU1	Ease1
		PEoU2	Ease2
		PEoU3	Ease3
		PEoU4	Ease4
		PEoU5	Ease5
Behavioral Intention	BIntention_Mean	BI1	Intention1
		BI2	Intention2
		BI3	Intention3
Innovativeness	Innov_Mean	Innov1	Innovativeness1
		Innov2	Innovativeness2
		REC_Innov3	Innovativeness3R
		Innov4	Innovativeness4

Table 7.1: Codebook

7.4 Appendix D

This appendix presents all remarks left by respondens of our survey.

7.4.1 Remarks fingerprint recognition

Scenario 1

- Having worked on a thesis closely related to this subject and technology directly aimed at breaking fingerprint sensors, using such simple sensors to authorize a transaction, when all they require is a pre-image and a malleable medium to transfer the fingerprint, sounds very dubious to me in terms of security. And, since there is no real requirement for phone manufacturers to opt for a fingerprint sensor that is immune to this issue, it'll probably keep on happening.
- Higher amounts are riskier in case you are hacked. more protection is needed for higher amounts.
- Wat mij zou tegenhouden is dat men onder dwang je vingerafdruk kan zetten.
- Bij hogere bedragen zou ik meer vertrouwen hebben in een ”two factor authentication”.
- Large amounts of transaction should have additional mode of validation.
- Ik zou het instellen tot een bedrag van 100,-
- Net als bij contactloos pinnen boven bepaald bedrag en na bepaald aantal keer inbouwen dat je dan weer je code moet invoeren.
- Instead of finger identification I use facial identification at this point in time
- Actually, I would like to be able to have both, password and fingerprint. In that case I will always be sure that everything will be fine with any action I should take care of at that time.
- Ik zou het willen gebruiken, maar mijn smartphone ondersteunt het niet

Scenario 2

- Looking over someone's shoulder to find out a pin number and stealing a debit card seems easier than chopping off a finger.
- Veel vragen worden onnodig gesteld “denkt je dat je makkelijk kan leren te bevestigen met vingerafdruk” “zou je het snel begrijpen” etc terwijl de eerste vraag al duidelijk was dat ik het allang gebruik
- I easily trust branded devices like Apple, Samsung, etc to store my fingerprint/personal data and access it for ease.
- Some questions have more nuance to it. I believe fingerprint authorization helps make processes faster and secure but for specific transactions, people should go through a multiple security check, especially big amounts or different location log-ins and unfamiliar transaction types and receivers. This would mean a combination of fingerprint and known password and OTPs.
- Ik heb niet zo zeer een probleem met de technologie, die is duidelijk in gebruik en best handig. Echter biedt het mij geen extra mogelijkheden boven

de functionaliteit die mijn bank-app op dit moment heeft: het voordeel is me niet duidelijk om een wachtwoord te vervangen door een vingerafdruk. Sterker nog, als ik slaap zou iemand potentieel met mijn vinger een transactie kunnen bevestigen, terwijl ze het wachtwoord niet zouden weten. De app zal de vingerafdruk ongetwijfeld versleuteld in de app hebben, maar alsnog geeft het me geen veilig gevoel... Om de zoveel tijd hoor je wel weer van een datalek, en dan slingert die informatie gewoon op straat. En stel dat ik ooit mijn hand verlies in een ongeluk o.i.d, wat dan? Wat mij betreft, doe maar niet.
– Omdat ik onvoldoende bekend ben met de vingerafdruk en alles wat er mee kan, heb ik bij veel vragen neutraal ingevuld.
– Ik zou eerder bereid zijn deze technologie in een tweestapsverificatie(bv code en vingerafdruk) te gebruiken dan alleen de vingerafdruk.
– Een gestolen wachtwoord kan je veranderen maar een gestolen vingerafdruk niet.

7.4.2 Remarks facial recognition

Scenario 3

– Depends on the amount.
– Als 2FA zie ik het wel als oke. Bijv. zoals de ING app heeft met een vingerafdruk + pincode. Los niet. Als 3 factor authenticatie zou het top zijn (optioneel).
– What if it's dark? It seems like a lot more work than biometric fingerprints.
– Ik vind de noodzaak om via gezichtsherkenning een transactie te doen nog niet aanwezig.
– Het nadeel van transacties voldoen via gezichtsherkenning is dat een gezicht bijna "publiek domein" is. We worden overal gefilmd en sturen foto's van elkaar rond. De enige die echt veilig met gezichtsherkenning kunnen bankieren zijn vrouwen die in het dagelijks leven boerka's dragen.
– I use my fingerprint to log in and confirm transactions. That's safe and less awkward than facial recognition. I wonder why I would need facial recognition as I don't feel there is any added value in comparison to using a finger print.
– I am still not entirely convinced that using face unlock/face ID is a safe way for doing financial transactions. Therefore, unless it becomes mandatory (fingerprint scanner disappears, which seems unlikely for now) I will not use it.

Scenario 4

– In het begin ben ik vrij enthousiast over het gebruik en de toepassing van gezichtsherkenning, echter naarmate het onderzoek vordert, wordt ik me steeds bewuster van de risico's die hieraan vastzitten. Scan van duim en/of code geeft toch nog het gevoel dat je niet zomaar kan inbreken in een account. Maar dat zal vast en zeker ook een schijngevoel zijn en even risicogevoelig als gezichtsherkenning (aanname).
– I would prefer a system with both facial recognition and a PIN.

- Zelf in te stellen max bedrag, net als nu met vingerafdruk of wachtwoord. Daarboven 2-factor identificatie.
- Er zijn toch andere biometrische kenmerken dan alleen gezicht om goedkeuring te geven? Bijv vingerafdruk. Ik zie niet waarom we met gezichtsherkenning moeten werken
- I seriously hope this is not the way of the future, I strongly believe that this method of payment can be easily manipulated especially with when it comes to the elderly.
- Mijn bezwaar is niet zozeer de techniek op zich, maar ik doe geen bankzaken via mijn telefoon. Mobiel gebruik van bankzaken vind ik nog de zwakke schakel. Gezichtsherkenning op zich kan goed werken.
- Methode is simpel maar hoge potentie voor misbruik bijv door foto's of hacken van frontcam
- For authentication purposes, I would opt for facial recognition like airport gate entry or opening my mobile device or computer or entry into restricted premises but definitely not for banking transactions.For financial transactions, I believe in personal feel and touch and being old school. Unfortunately its my behavior trait.

7.4.3 Remarks pattern recognition

Scenario 5

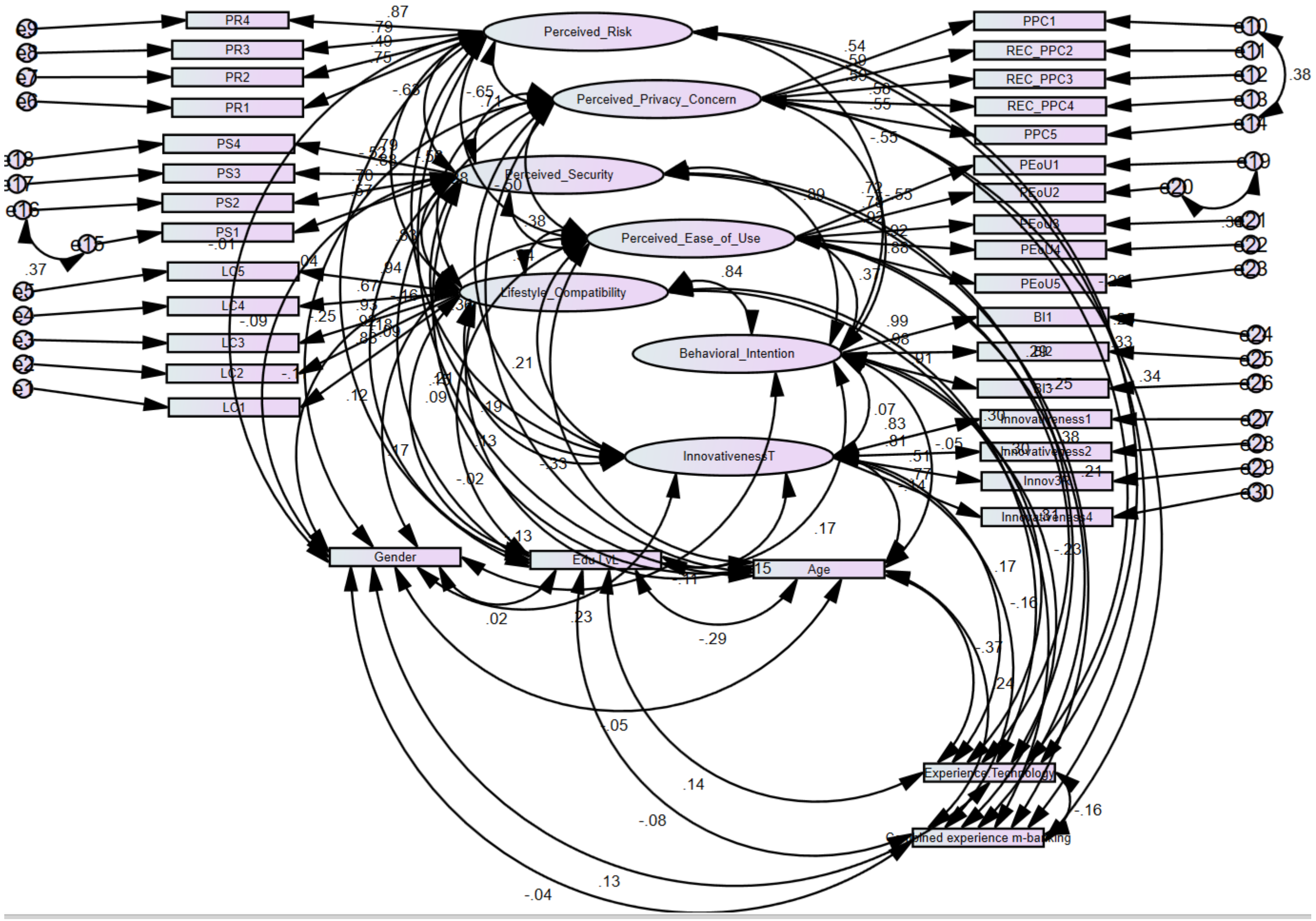
- Veel dezelfde vragen anders geformuleerd (misschien expres), maakt de enquête beetje saai op den duur Het is mij niet duidelijk was het voordeel is van een patroon tekenen ipv 5 cijfers intoetsen. Een patroon blijf je soms in vegen zien op het scherm en is ook makkelijker voor anderen om te zien wanneer ingevoerd, wat het dus gevoeliger zou maken om misbruikt te worden. Het is nauwelijks sneller en zit op hetzelfde niveau van gebruikersvriendelijkheid naar mijn mening. Ik was al heel sceptisch over mobiel bankieren, dus dit zal ik niet snel gebruiken. Wellicht zou een maximum bedrag voor patroonherkenning dat gevoel verminderen.
- wellicht hack gevoelig. niet beveiligd genoeg
- Er is weinig verschil in de level of assurantie tussen wachtwoorden en patroonherkenning voor mij. Wat ik zoek is second factor authenticatie waarin patroonherkenning een factor kan zijn.
- ING kent al bevestiging via vingerafdrukscanner. Dat is voor mij makkelijker dan een patroon. Het gaat mij om gemakzucht, vandaar lage kant dat ik met een patroon ga werken.
- Ik denk dat mobiele patroonherkenning risico's met zich meebrengt op het gebied van security en privacy. Een dubbele check zou mijn voorkeur hebben, dus bijv patroon en wachtwoord
- I do not see a clear benefit compared to PIN or wireless. If it would replace an identifier, it see a benefit, but that has nothing to do with a pattern.
- We leven nu in een digitale wereld dus dit is normaal voor ons, bijna alle informatie voor en over iedereen is beschikbaar op internet. Het geeft mij niet perse een veilig gevoel maar meer omdat je het gewend bent is het normaal

- None of my financial services offers this service Would only use it for smaller amounts - larger amounts would need more verification
- Bij een te hoge bedrag zou ik liever naar de bank willen gaan dan middels deze technologie. Voor een bedrag tot 1500,- euro zou ik het wel willen gebruiken.

Scenario 6

- Ik vind een vingerafdruk scanner een veel betere en veiligere manier om middels een mobiel apparaat betalingen goed te keuren.
- Combineren van authenticaties heeft de toekomst.
- Laat anderen het maar uitproberen, we lezen de ”zielige” verhalen van geplunderde rekeningen wel. Patronen zijn makkelijk op afstand te herkennen.
- I would use fingerprint recognition, but not pattern recognition.
- Het lijkt mij geen goede manier doordat de lijn van je patroon zichtbaar is op het scherm.
- Biggest risk I see: tampering with the pattern by criminals biggest competitor for authentication I see is fingerprint and facial/iris recognition.
- Ik heb liever vingerafdruk/vingerscan
- Ik zou deze technologie best willen gebruiken. Maar ik gebruik al pin en vingerafdruk verificatie via een mobiele bank-app bij online aankopen, en ik vraag me even af hoe patroonherkenning veiliger of anders is dan verificatie via pin of vingerafdruk? Wat is de toegevoegde waarde, in termen van gemak, snelheid of beveiliging?

7.5 Appendix E


Perceived_Risk
Perceived_Privacy_Concern
Perceived_Security
Perceived_Ease_of_Use
Lifestyle_Compatibility
Behavioral_Intention
InnovativenessT
Gender
Edu Lvl
Age
Experience Technology
Gained experience m-banking
PR4
PR3
PR2
PR1
PS4
PS3
PS2
PS1
LC5
LC4
LC3
LC2
LC1
PPC1
REC_PPC2
REC_PPC3
REC_PPC4
PPC5
PEoU1
PEoU2
PEoU3
PEoU4
PEoU5
BI1
BI2
BI3
Innovativeness1
Innovativeness2
Innov3
Innovativeness4
e1
e2
e3
e4
e5
e6
e7
e8
e9
e10
e11
e12
e13
e14
e15
e16
e17
e18
e19
e20
e21
e22
e23
e24
e25
e26
e27
e28
e29
e30
.87
.79
.40
.75
.37
-.01
.04
-.09
.25
-.65
-.65
.71
.54
.59
.58
.56
.55
-.55
.80
.72
-.53
.92
.88
.37
.84
.38
.94
.67
.93
.21
.99
.98
.91
.07
.83
.81
-.05
.51
.77
-.33
.34
.33
.25
.38
.21
.19
.13
-.02
.17
.12
.09
.13
.15
-.11
.02
.23
-.29
.05
.14
-.08
.13
-.04
.17
-.16
-.37
.24
-.23
-.16
.38