ISCTE IUL

Instituto Universitário de Lisboa

Department of Social and Organizational Psychology

"In God we trust, all others we scan for malware": A study on the effect of trust in using AI empowered smartphones.

Miguel Ângelo Agostinho Longle

Dissertation submitted as partial requirement for the conferral of Master in Social and Organizational Psychology

Supervisor:
Doutor Nelson Campos Ramalho
Assistant Professor, ISCTE-IUL

September 2019

ACKNOWLEDGMENTS

After 6 long years through my academic journey, I can say I am proud of my achievements as a student, and of my growth, both as a student, and colleague, and I feel all culminates on this final work, of which I am particularly proud of. It is the end of an era, and I feel it could not have ended in a better way.

But I could not have done it alone. So, I would like start by thanking all the participants that allowed this dissertation to be possible. Thank you all for your time and patience, and willingness to help me get through this entire process.

I would also like to thank my family members, and Carlos Caldeira for taking time to help me with this dissertation, but also for all the support they gave me thorough my life. Also, very special thanks to my friends Clara Rodrigues, Duarte Moreira, Bruno Baixinho, Iris Pereira and Rodrigo Carvalho, for the patience and support, for keeping me sane thorough this ordeal and for being there for me no matter what, proving that friends are indeed the family we get to pick.

I could not end this dissertation without thanking Professor Nelson Ramalho, not only for all time and patience he had with me, but also for the guidance, for sharing his unending wisdom and energy and all the “so crazy it might work” brainstorming ideas I could have possibly imagine. So, thank you.

Last but definitely not least, I would like to thank the most important people on my life. I want to thank my mother and my father for shaping me into the man I am today, and for being there for better and for worse. To my girlfriend Sara, thank you for all the love and support and for being my rock these past 5 years.

RESUMO

A aceitação de novas tecnologias é um assunto importante na investigação organizacional que tem um longo passado de teorização. Modelos tais como o C-TAM (Bruner & Kumar, 2005) têm sido propostos para explicar a intenção de usar tais tecnologias. Contudo, tais modelos foram desenvolvidos antes da incorporação da Inteligência Artificial (IA), um dos temas mais recentes e entusiasmantes da sociedade atual, cujas aplicações aumentam de dia para dia. A introdução desta nova tecnologia mudou substancialmente o estatuto da tecnologia no que concerne ao seu impacto potencial e á influência subtil na livre escolha. A penetração que a tecnologia potenciada pela IA tem ganho através dos smartphones é um dos fenómenos que merece atenção, especialmente face às opiniões controversas emitidas por personalidade líderes na ciência e tecnologia como Stephen Hawking e Elon Musk relativas ao tópico da confiança.

Este estudo procurou testar o papel da confiança como mediadora entre o C-TAM e a intenção de utilizar aplicações potenciadas com IA. Com uma amostra de 211 utilizadores de smartphone, os resultados mostraram várias mediações totais, salientando o papel fundamental que a confiança desempenha na implementação bem-sucedida desta tecnologia.

Palavras-chave: Confiança; Inteligência Artificial; C-TAM; Intenção de uso

ABSTRACT

The acceptance of new technologies is an important subject in organizational research that has a long past of theorizing. Models such as C-TAM (Bruner & Kumar, 2005) have been proposed to explain the intention to use such technologies. However, such models were developed prior to the incorporation of Artificial Intelligence (AI), one of the latest and most exciting themes in today's society, whose applications increase from day to day. The introduction of this new technology has substantially changed the technology's status regarding its potential impact and subtle influence on free choice. The penetration that AI-powered technology has gained through smartphones is one of the phenomena that deserves attention, especially in the face of controversial opinions from personality leaders in science and technology like Stephen Hawking and Elon Musk on the topic of trust.

This study sought to test the role of trust as a mediator between C-TAM and the intention to use AI-enhanced applications. With a sample of 211 smartphone users, the results showed several total mediations, highlighting the key role trust plays in the successful implementation of this technology.

Keywords: Trust; Artificial Intelligence; C-TAM; Intention of use

TABLE OF CONTENTS

Contents

List of Tables

List of Figures

List of acronyms

TAM – Technology Acceptance Model

EoU – Ease of Use

BI – Behavioral Intention

IT – Information Technology

C-TAM – Consumer Technology Acceptance Model

CFI – Comparative Fit Index

TLI - Tucker-Lewis Index

RMSEA – Root Mean Square Error of Approximation

CR – Composite Reliability

CFA – Confirmatory Factor Analysis

AI – Artificial Intelligence

Introduction

Artificial Intelligence (AI) is one of the newest and most exciting themes in today's society. As this new technology keeps evolving, we are now entering an Era that focus on intelligence, not only from a human perspective, but also from a more mechanical one, with new artificial agents entering the fray, capable of performing activities with a Human-like performance. However, despite being used to improve fields like medicine, investigation, healthcare, and so many others, AI is also present in our daily lives, via applications and gadgets, namely smartphones, which use AI powered applications (or apps). These gadgets and their apps made us start looking at AI from a consumer point of view, since smartphones are now widely accepted and used all around the world.

However, recent development shows that these AI powered gadgets came with certain risks, such as unwillingly sharing personal or banking information, or our physical location with ill-intended third parties, be it through the usage of apps or through safety breaches and data leaks exploited by harming AI powered software.

So, what makes us keep using them? With the added risks of using AI powered gadgets, we recognize that it is essential to assess people’s trust towards AI and its relation with people’s acceptance and use of this new technology, adding a trust component to the already established C-TAM model (Bruner & Kumar, 2005).

The structure of this dissertation will focus on the aspects mentioned above, in order to provide knowledge regarding this theme and, hopefully, relevant conclusions. In Chapter I we will begin contextualizing the already existing literature, highlighting the definition of AI, and its application areas, with special focus on smartphone devices. We will then take a look at trust, highlighting its definition and current state, both from an interpersonal and also an AI-focused perspective. Lastly, we will talk about technology acceptance and highlight both TAM (Davis, 1986) and C-TAM (Bruner & Kumar, 2005) models.

Chapter II will describe the methodologies used in the present study, clarifying the variables studied as well as the procedure steps.

Finally, Chapter III will report the results of the conducted analysis, which will be further discussed in Chapter IV. This last chapter will also mention limitations occurred in the present study and provide suggestions for future studies.

Chapter I – Literature Review

Literature review will cover the main subjects and their relationships namely by defining AI and its applications, the specific case of smartphones and embedded AI and ensuing trust they receive from users. To offer a comprehensive framework, literature review will also explain the technology acceptance model by David (1986) and its revised C-TAM model (Bruner & Kumar, 2003) and the hypotheses that stem from it.

1.1. Artificial Intelligence: Definition and Applications

AI as a concept was introduced by John McCarthy in a conference in Dartmouth in 1956 (Copeland, 1993; Russel & Norvig, 1995), and is considered a subdivision of computer science with the main goal of programming computers and creating systems that would previously require human intelligence to operate (Gips, 1979; Ertel, 2017). It uses symbolic reasoning and sophisticated knowledge structures and techniques so that the system's performance can be analogous to human learning and decision-making (Atkinson, 2016; Hillman, 1985; Russel & Norvig, 1995). It is characterized as a field of research that develops intelligent agents using deep and machine learning techniques to ease interactions between humans and machines/technology (Atkinson, 2016; Lisetti, & Schiano, 2000). According to Spiegeleire, Maas and Sweijs (2017), there are also three tiers of AI:

- **Artificial Narrow Intelligence** (ANI or "narrow/weak AI") refers to machine intelligence that is restricted to specific tasks, equaling or exceeding human intelligence. Examples of this would be systems like Google translate or specialized automatic systems like smartphone applications (or apps);
- **Artificial General Intelligence** (AGI or "strong AI"), which is an advanced level of AI meeting the full range of human performance on any task;
- **Artificial Superintelligence** (ASI) is the pinnacle of AI, where it excels human intelligence and performance in any task or field.

1.1.1. AI Applications

AI is a complex subject that embraces several fields (Gips, 1979; Hillman, 1985; Russel & Norvig, 1995, Hengstler, Enkel & Duelli, 2016). Depending on the specifications of each field, it can take many names such as machine learning, machine intelligence, deep learning, and cognitive computing (Atkinson, 2016). However, even though there are AI application areas with different characteristics, they should not be dissociated from each other, since most of AI systems are a merge of several AI fields. Here we intend to explore some of the more relevant fields where AI systems are present.

Expert systems: These systems work with a combination of a theoretical understanding of a certain problem and several heuristic problem-solving rules regarding that problem (Luger, 2009; Pannu, 2015). These systems use programs that work within a certain specialized domain (Copeland, 1993; Hillman, 1985; Luger, 2009), like reading Biometrics (Xiao, 2007), preventing cyber assaults (Anwar & Hassan, 2017) or performing medical diagnoses (Agha, Jarghon & Naser, 2017; Hillman, 1985; Luger, 2009).

Natural Language Understanding: Another relevant field for AI systems is natural-language understanding (Brent, 1988; Hillman, 1985; Nilsson, 2014), which refers to programs that can process, read, and analyze natural language input. Examples of its application include machine translation, which translates texts from one language to another; speech understanding; holding intelligible conversations using bots, and answering questions (Gips, 1979; Hillman, 1985).

Robotics: Finally, we have the field of robotics. This field agglomerates a spectrum of disciplines besides AI, such as mechanical engineering, industrial engineering, computer science, physics, materials science, manufacturing systems engineering, and control theory (Hillman, 1985). The difference from the other areas is that robots are mobile and can manipulate objects (Gips, 1979; Luger, 2009; Nilsson, 2014; Pannu, 2015). Examples where robots have been applied successfully include: healthcare (Robinson, MacDonald & Broadbent, 2014), education (André, Baker, Hu, Rodrigo & Boulay, 2017), transportation/navigation and industrial automation (Pannu, 2015), and many others.

1.1.2. The smartphone as an AI Gadget

It is a well-known fact that most smartphones contain some version of AI, such as speech recognition (Atkinson, 2016), but how did we get here? In the beginning of mobile technology development, mobile phones were devices mainly used by middle and upper-class people (Lacohee, Wakeford, & Pearson, 2003). However, as they evolved, new features have been added, such as full color screen, texting, mp3 function, embedded camera, and access to the internet. Mobile phone's development has shown a trend towards getting smarter and more user-friendly (Yu, 2012), hence the new term "smartphone". A smartphone is a mobile phone that offers more advanced computing ability and connectivity than a contemporary basic feature phone. Smartphones run complete operating system software providing a platform for application developers (Mulliner, 2006). With this feature, smartphone users can develop programs which are customized in specific needs, which is an advantage. This allows smartphone users to search restaurants, nearest train stops, and pretty much anything like you could with a computer. Furthermore, a smartphone user can trade their assets like stocks or use banking service with wireless network and send or receive e-mails, too (Jeon, Kim, Lee & Won, 2011). Smartphones and tablets connected to the Internet through Wi-Fi have also influenced social interactions to a significant extent through AI applications to the point of reaching about 61% of people on their daily lives (Makridakis, 2017). However, this comes with a cost: the amount of personal information that we put into our smartphones. Inside, we can find phone call logs with information about placed and received calls, browsing history about visited web sites, as well as cached emails and photos taken with the built-in camera. As these are all private information, a natural concern is the safety of these data (Zhou, Zhang, Jiang & Freeh, 2011)

1.1.3. Smartphone Security

Recent studies (e.g. Abubaker et al., 2018; Egele, Kruegel, Kirda & Vigna, 2011; Enck, Gilbert, Chun, Cox, Jung, McDaniel & Sheth, 2010; Mahaffey & Hering, 2010; Talal et al., 2019) showed that there are malicious apps on the market that can be uploaded to the app stores and then successfully advertised to users for installation on their smartphones. These apps have shown to leak private information without user authorization (Zhou et al., 2011). Which makes it crucial to users to understand how safe their mobile devices are. Mobile device security has five key aspects that distinguish it from computer security (Mulliner, 2006):

- **Mobility**. Mobile devices are, by definition, mobile, so they are not kept in one place therefore, they might be stolen and/or tampered with.
- **Strong Personalization**. Mobile devices are normally not shared between several users, unlike computers, so, they are kept close to their owners.
- **Strong Connectivity**. Many devices support ways to connect to the Internet.
- **Technology Convergence**. Mobile devices combine many different technologies, such as a mobile phone, a music player, and a camera in a single device.
- **Reduced Capabilities**. Mobile devices such as smartphones are computers but lack many features that desktop computers have. For example, a mobile device does not have a full keyboard and has limited processing capabilities.

This suggests that mobile devices' security is more complex than a computers' security (Mulliner, 2006).

Mobility increases the risk of data theft, since it is easier to steal a mobile device than break into a computer. Strong Personalization together with Strong Connectivity increases the threat of privacy violations, like locating the owner by locating the device. Technology Convergence leads to additional security risks because every additional feature adds a new target that can be attacked. Reduced hardware capabilities may facilitate certain kinds of Denial-of-Service attacks, rendering a device temporarily unusable. In addition, missing features, like the lack of a full keyboard, makes it harder to implement effective authentication mechanisms (e.g., username and password) (Mulliner, 2006).

1.2. Trust

Trust is arguably the most critical concept in studying human social interactions and has been an important construct in personality and in helping understanding development, communication, personal relationships, and organizational behavior for a long time (Couch & Jones, 1997). As a psychological state, trust is composed of two interrelated cognitive processes. The first being a willingness to be vulnerable to the actions of another party, and the second referring to maintaining a positive expectation regarding the other party's intentions, motivations, and behavior, despite being uncertain about how the other will act (Lewicki, Tomlinson & Gillespie, 2006).

Previous work on trust contains a diversity of definitions and conceptualizations and has been defined in several ways. Earlier definitions of trust (e.g., Deutsch, 1958; Rotter 1967) often defined it as trust in human nature or people-in-general, whereas recent approaches focus on trust in a specific partner, often romantic (termed relational trust; Larzelere & Huston, 1980; Rempel, Holmes, & Zanna, 1985).

The concept of a global trust is approached by Julian Rotter (1971) who focused on what he called ''interpersonal trust'' which refers to a generalized expectancy that the promise of an individual or a group can be relied upon.

On the other hand, relational trust differs from the idea of global trust since it is focused on a specific partner with whom a person shares a relationship (Holmes, 1991; Holmes & Rempel, 1989). It refers to a person's level of confidence in the strength of the relationship and his/her partner's positive feelings (caring) toward the person (Rempel et al., 1985). The concept of relational trust has been almost exclusively used to refer to trust in romantic partners (Couch & Jones, 1997).

According to research (Lewicki et al., 2006), trust is a multifactorial state that includes cognitive, affective, and behavioral intention subfactors. That is, trust is deemed to be a single, superordinate factor, with cognitive, affective, and behavioral intention subfactors.

The cognitive subfactor refers to the beliefs and judgments about another's trustworthiness and is the most emphasized in prior research on trust (Lewicki et al., 2006). This means that people cognitively choose whom they trust in which respects and under which circumstances, basing the choice on what they consider to be evidence of trustworthiness (Lewis & Weigert, 1985). However, since trust only exists if there is a risk involved (Mayer, Davis & Schoorman, 1995), trustors do not know with absolute certainty how the trustee will act. Thus, the cognitive basis of trust reduces uncertainty by providing a foundation from which people can judge whether we can trust someone (Lewis & Weigert, 1985).

The emotional subfactor of trust shows that there is often an emotional bond between the parties, especially in close interpersonal relationships (Lewis & Weigert, 1985). Therefore, the emotions experienced in a trusting relationship with another person, be it outrage at trust violations or as affection toward an intimate partner, are likely to affect the cognitive subfactor of trust which then affects how trust is established and sustained (Lewis & Weigert, 1985).

The behavioral-intention subfactor of trust refers to someone acting, on the confident expectation (cognitive basis) and feelings (emotional basis) that the other will honor trust. It is through trusting behavior that we demonstrate our willingness to be vulnerable to the actions of others (Lewicki et al., 2006). Research shows that when we trust others, they become more likely to behave in a trustworthy manner and to trust us in return (Lewicki et al., 2006). Research also show that, the outcome of trusting behavior (i.e., whether trust was well placed or not) provides information that will reinforce or change whether someone is trustworthy or not (Mayer et al., 1995).

Although much is known and has been theorized about human trust, the target of trust has been mainly a social target, i.e. another person, a social construct such as an institution or human-based actions. However, trust can target non-social entities such as a machine or an algorithm.

1.3. Trust in AI

Flying on a plane, relying on the auto-pilot to get us to our destination safely, undergoing laser eye surgery and trusting the system will be able to decide correctly how to perform surgery or being driven by an automatic car system are all examples of how much we need to trust in AI on our daily lives. Trust in these systems comes from the confidence that they will not fail (Hind, Mehta, Mojsilovic, Nair, Ramamurthy, Olteanu, & Varshney, 2018). Although AI services are achieving impressive accuracy in many application domains where it may suffice in certain areas, deployments of AI in critical decision-making applications, like credit applications or medical recommendations, require greater trust in AI (Hind et al., 2018). Like any new technology, trust in AI is determined by human characteristics, environment characteristics, and technology characteristics (Siau & Wang, 2018).

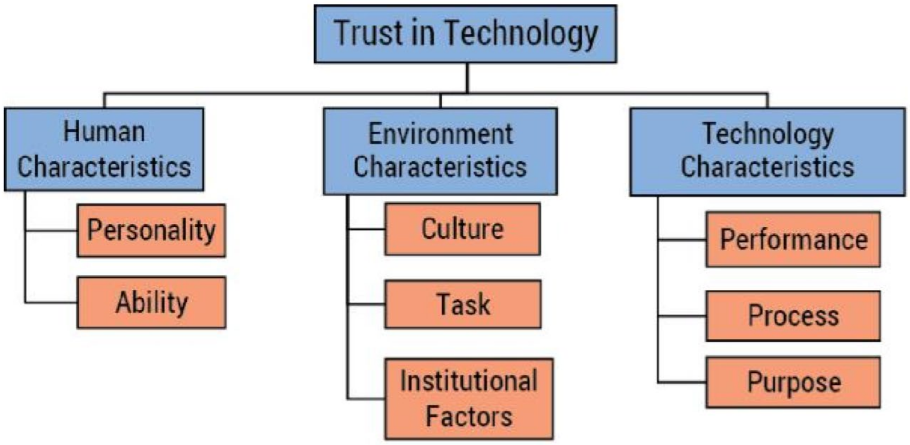

Figure 1.1 - Factors and dimensions of trust in technology (Siau & Wang, 2008: 50)

Human characteristics are unique to each individual and can refer to ability-based factors and personality-based factors (Oleson, Billings, Kocsis, Chen, & Hancock, 2011). Ability-based factors refer to the cognitive aspects of trust, which includes experience or expertise acquired through using new technologies (Muir, 1994). According with the same author, both experience and expertise mean that the user is receiving information about the system, which can help the individual predicting the system's behavior, making it more trustworthy. Personality-based factors refer to an individual's feelings and personality. Research about the most important personality-based factors of trusting AI focus upon an individual's predisposed tendency to trust others (Lee

& See, 2004; Oleson et al., 2011). This dispositional trust is influenced by the user's different experiences, personality traits, and cultural backgrounds (Siau & Wang, 2018).

Environment characteristics will vary according to the contexts where AI is used but mostly refer to the cultural background, to the nature of the tasks and institutional factors (Siau & Wang, 2018). Cultural context influences trust through social norms and expectations (Lee & See, 2004). Wang, Rau, Evers, Robinson, and Hinds (2010) found support that culturally normative behavior by a robot can influence participant's behavioral responses to robot collaborators due to higher levels of trust. Also, Wang et al. (2010) discovered that cultural values, like individualism vs. collectivism, explains attitudes towards robots. Tasking characteristics refer to how complex or demanding the tasks assigned are and how it affects trust in AI, as more complex and demanding tasks are shown to have different effects in developing trust than less demanding tasks (Oleson et al., 2011). Adams, Bruyn, Houde, Angelopoulos, Iwasa-Madge & McCann (2003) theorized that trust might decrease with more demanding tasks, since there is more room for error. Institutional characteristics refer to how trust can be generated based on institutional structures (Li, Hess, & Valacich, 2008). Zucker (1986) suggested institutional characteristics are especially relevant in situations where there is no previous interaction between the trustor and trustee. According to research, there are two Institutional characteristics responsible for generating trust: situational normality and structural assurance (Lewis & Weigert, 1985; McKnight et al., 2002). Situational normality refers to when the situation is normal and all is in proper order (Lewis & Weigert, 1985). This means that if the trustor has no knowledge about the trustee, the trustors will rely on their feelings about the situational setting in order to build trust (McKnight et al., 1998). This means people are more likely to trust someone in a normal and anticipated setting (Baier, 1986). Structural assurance refers to safeguards, like promises, contracts, regulations, and guarantees that are set in place in order to help create trust (Shapiro, 1987; Sitkin, 1995). Research shows that Legal safeguards like regulations, laws, and contracts help strengthen the trustor's beliefs that the trustee will fulfill the promise they made to the trustor (Sitkin, 1995). In a more AI-centric context, these safeguards appear under the form of encryption, specific system development processes and procedures (McKnight and Chervany, 2000), feedback mechanisms (Pavlou and Gefen, 2004) and third-party certifications (Luo, 2002). Overall, research has shown that when solid institutional structures are in place and the social environment is in order, trustors are more likely to grant trust in general (McKnight, Cummings & Chervany, 1998) which can be interpreted as stability granted by institutional settings being taken as a facilitator of trust.

Finally, technology characteristics comprise three dimensions: performance, process, and purpose (Lee & Moray 1992; Siau & Wang, 2018). Performance rests on expectation that the system will act stably and consistently to perform what it is intended to (Lee & Moray 1992). Hengstler, Enkel and Duelli (2016) identified two determinant factors for performance trust: operational safety and data security. To guarantee operational safety, a technology must be certificated and approved, and policies established to govern it (Hengstler et al., 2016). To assure data security, standards must be set in place and when dealing with personal data, it is essential to provide information about how the data is used and who can access it (Paluch & Wunderlich, 2016). Process refers to how the system operates and refers to its intelligibility (Lee & See, 2004). Hengstler et al. (2016) named three categories associated to process trust: cognitive compatibility, trialability, and usability. Cognitive compatibility is a major determinant of the process dimension of trust. If the algorithms are understandable and guide users towards achieving their goals, they tend to trust the system (Hengstler et al. 2016). Trialability is an additional strategy to enhance understanding, as trials were found to reduce concerns of both potential users and the media (Hengstler et al. 2016). Usability is another determinant for the process dimension of trust in the technology. The interfaces need to be designed in a way that the system can be easily and intuitively used, but it also must mediate between control and autonomy. It also must first prioritize the characteristics of the end-user, such as age and context of use (Hengstler et al. 2016). Lastly, Purpose, as the third determinant of trust in technology, describes why the system was developed (Lee & Moray 1992). To ensure Purpose trust, any new system needs to be placed into a defined context, by explaining the purpose of the system. This is necessary to avoiding generalizations and helping promote trust (Hengstler et al. 2016).

Overall, Trust is a critical issue in dealing with technology whatever its nature. It is necessary to actually use it and to see it as useful, easy to use, eventually fun. However, the emergence of AI and the moral judgment it entails adds another dimension: that of benevolence. The most used model on technology acceptance is TAM (Davis, 1986) and even in its more updated form (e.g. C-TAM Bruner & Kumar, 2003) it does not cover this moral dimension.

1.4 Technology Acceptance Model

The TAM model (Davis, 1986) has been used for years to predict behaviors and attitudes of employees as they are introduced to new technologies in the work space (e.g. Abdalla, 2007; Sanchez & Hueros, 2010; Pando-Garcia, Periañez-Cañadillas & Charterina, 2016; O'Dell & Sulastri, 2019). The model states that usefulness and ease-of-use of a system influences a person's intention to use the system. There have been several versions of the model proposed over time in the workplace context. The key difference between workplace and consumer contexts when it comes to TAM is that, a hedonic factor may be an important addition to the model when we add a consumer context (Childers et al., 2001; Dabholkar and Bagozzi, 2002). This results in c-TAM (consumer technology acceptance model) (Bruner & Kumar, 2003).

A hedonic dimension has been explored in consumer behavior, as reflected in C-TAM (Bruner & Kumar, 2003) and it relates with trust because trust has an affective dimension (McAllister, 1995; Jones, 1996). Cognitive and affective trust are not independent dimensions (Autor) and they contribute in a twofold path to decision making, pertaining uncertain outcomes. For example, Punyatova (2019) explored how cognitive and affective trust impacted online customer behavior and found that both mediated the relationship between website characteristics and customer satisfaction. The choice for a single overarching trust scale that encompasses both cognitive and affective dimensions might be preferable within a technological focused research because difficulties may arise in using them separately as illustrated by Punyatova (2019) coefficient values between affective and cognitive trust that fall out of technical requirements.

Considering the overall relations already known in C-TAM (Bruner & Kumar, 2003) as well as the assumed influence they may play in building trust in AI-based smartphones we establish a set of hypotheses.

Hypothesis 1 concerns the relationship between easy-of-use and trust via usefulness and fun. Therefore, we hypothesize that:

> Hypothesis 1a: **Usefulness** mediates the positive relationship between **easy-of-use** and **trust**
>
> Hypothesis 1b: **Fun** mediates the positive relationship between **easy-of-use** and **trust**

Hypothesis 2 concerns the mediating role trust plays between CTAM components and behavioral intentions. Therefore, we hypothesize that:

> Hypothesis 2a: **Trust mediates** the positive relationship between **usefulness** and **behavioral intention** to use biometrics-related apps (2a.1), money-related apps (2a.2), social-related apps (2a.3) or health-related apps (2a.4).
>
> Hypothesis 2a: **Trust mediates** the positive relationship between **fun** and **behavioral intention** to use biometrics-related apps (2a.1), money-related apps (2a.2), social-related apps (2a.3) or health-related apps (2a.4).

Hypothesis 3 concerns the full sequential mediational path linking easy-of-use to behavioral intentions. Therefore, we hypothesize that:

> Hypothesis 3a: **easy-of-use** is positively related to **behavioral intention** to use smartphone apps through a sequential indirect effect via enhanced **usefulness** and subsequent **trust.**
>
> Hypothesis 3b: **easy-of-use** is positively related to **behavioral intention** to use smartphone apps through a sequential indirect effect via enhanced **fun** and subsequent **trust.**

The set of hypotheses are integrated into the following research model (Figure 1.2).

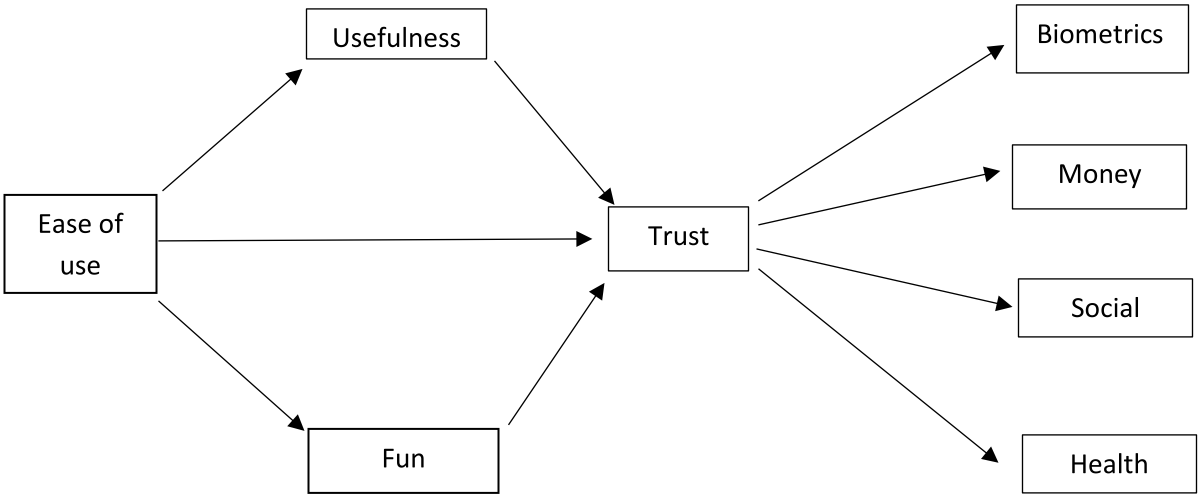

Figure 1.2 - Research model.

Chapter II – Method

2.1. Procedure

The questionnaire (Annex A) for this work was shared online through social media, like Facebook, LinkedIn and in academic groups. Firstly, there was a brief introduction about the study, where the participants would learn about its conditions and also, were given some relevant information about the study. The participants would then give, their informed consent, if they agreed with them. Otherwise, the study would end. The Participants would then be asked some questions about possible control variables (e.g., "Do you have a smartphone?", "How long have you had a smartphone?"; “To what extent do you consider that your smartphone incorporates artificial intelligence?"). Next, participants would answer some questions about Trust in their smartphone devices using Reid &Levy’s trust scale (2008) composed by items on a Likert scale (1 = “*Strongly Disagree*”; 5 = “*Strongly Agree*”). Then, the questionnaire would follow with the behavioral intention of use items, measured through c-TAM (Bruner & Kumar, 2005) on a Likert scale equal to the Trust scale, which measures Usefulness, EoU and Fun. Finally, the participants would be asked sociodemographic questions in order to characterize the sample, such as age, gender, literacy, marital status and about their profession, whether it was It related or not. In the end, the participants would receive a “thank you” message and the questionnaire would end.

2.2. Sample

A sample of 211 individuals was gathered for this study, of which 70.8% are female. The participants ages ranges between 18-69 years-old, with an average of 30.16 years-old (sd=11.73). On Marital Status, a larger portion of individuals are single, representing 72.8% of the total sample.

Some control variables were included in the study to determine if they have an effect on the relationship between the independent and dependent variables. These include a question about whether the participants profession relates to the IT field (dummy coded 1=Yes and 2=No), which showed that 79.2% of participants do not have a profession related to this technological area. Another added variable is the smartphone usage (dummy coded 1=Yes, and 2=No) which individuals stated to occur from 1 to 24 years, averaging 6.9 years (sd=3.5). The results also showed that the average percentage of individuals using a smartphone is 69.9% (sd=11.73). Awareness of AI features in own smartphone was measured using a Likert scale (1=does not incorporate anything close to AI" to 7 "Incorporates a lot of AI, even more than people think"), and the mean was 4.98 (sd=1.46).

2.3. Data analysis strategy

Data analysis followed a twofold strategy where variables were tested for their psychometric quality (i.e. that they are both valid and reliable) and then, after guaranteeing these conditions, the analysis focused on hypothesis testing.

A given measure is considered psychometrically sound when it has good fit indices in a Confirmatory factor analysis, and cumulatively has both convergent and (when applicable) divergent validity. A confirmatory factor analysis goodness of fit is judged on the basis of indices as proposed by Hair et al. (2010) as follows: χ^2/df below 3.0 and with a non-significant p-value, Comparative Fit Index (CFI) above .92, Tucker-Lewis Index (TLI) above .92), Root Mean Square Error of Approximation (RMSEA) below .06. This indicates construct validity. Additionally, the measures are expected to comprehend factors that have convergent validity, i.e. where average item loading achieve at least 50% variance, which means the Average Extracted Variance (AVE) should be .50 or higher. Also, whenever the factor solution counts with more than a single factor, divergent validity should be tested. It is expected that a solution with divergent validity show higher average factor loadings in each factor than the respective interfactor correlations. Lastly, measures are expected to be reliable, i.e., either show a Cronbach alpha or a Composite Reliability of .70 or higher. According with Fornell and Larcker (1981: 46) whenever AVE fails to reach the threshold, we can judge the suitability of the factor based on CR's threshold. Common method/source bias (Podsakoff et al., 2003) can be tested via a single latent variable in SEM analysis.

Hypothesis testing was conducted with Structural Equations Modelling using AMOS 24. We designed the model by incorporating all latent variables and respective observed items coupled with errors. As recommended by Hayes (2017) we conducted a bootstrapping with 5000 repetitions for a bias corrected CI95. As a rule, coefficients are considered significant if the value zero is not comprehended in the lower and upper confidence interval values. Model fit was assessed with the same fit indices used for CFA (Hair et al., 2010).

2.4. Measures

Behavioral intention of use was a measure built for this study on the basis of a focus group that was built to understand the range of applications usable with a smartphone. Participants were requested to state in a 5 point item scale (1=”never”, 5=”always”) their intention to use categories of application. In its original design it comprehended 15 items covering five groups of smartphone applications use, namely: 1) money-related (3 items, e.g. online banking), 2) social contacts related (4 items, e.g. social networks), 3) health-related (2 items, e.g. health status monitoring), 4) biometrics related (4 items, e.g. fingerprint access), and 5) GPS related (2 items, e.g. tracking on base of GPS). By conducting a CFA with this solution we found the fit indices unsuitable ($\chi^2/82$=2.237, *p*<.001; CFI=.897, TLI=.849, RMSEA=.077). By using Lagrange multipliers as well as applying rules for psychometric quality as stated in section “Data analysis strategy” we excluded several items and the final factorial solution kept four of the five initial factors. The resulting model showed good fit indices ($\chi^2/31$=1.323, *p*=.108; CFI=.984, TLI=.972, RMSEA=.039) and the structure of the factors is the following: 1) money-related (3 items, “Int1_Colocar os meus dados pessoais numa aplicação do smartphone”, “Int2_Aceder à minha conta bancária”, and “Int11_Usar aplicações que exigem um cartão de crédito”, AVE=.468, CR=.72), 2) social contacts related (3 items, “Int8_Aceder ao email pessoal”, “Int7_Aceder a uma rede social”, and “Int3_Guardar fotos pessoais”, AVE=.43, CR=.70), 3) health-related (2 items, “Int4_Guardar ou permitir a monitorização do meu sono” and “Int6_Usar aplicações de monitorização da minha saúde ou alimentação”, AVE=.52, CR=.69), and 4) biometrics related (2 items, “Int14_Usar identificação biométrica pela retina ou iris” and “Int15_Usar reconhecimento facial”). It has good convergent validity (AVE=.89) as well as reliability (CR=.94).

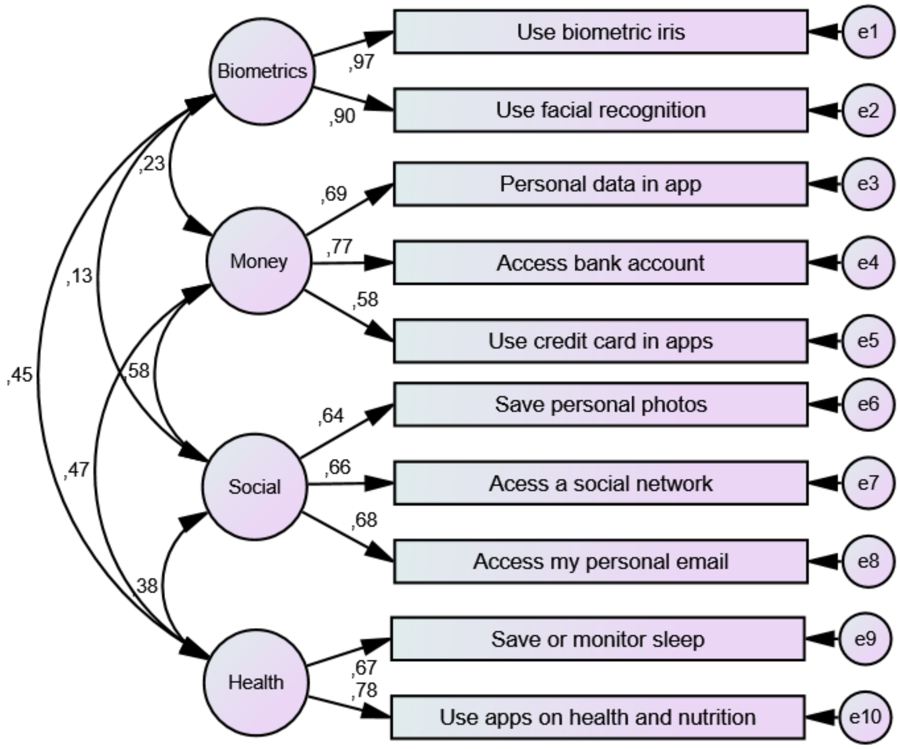

Figure 2.1 – CFA for behavioral intention to use apps

Technology acceptance was measured with C-TAM that comprehends three dimensions: ease of use (EoU, 5 items, e.g. “I quickly learned how to use it”), usefulness (5 items, e.g. “Requires a lesser number of steps to do the tasks I want to”), and fun (6 items, e.g. “dissatisfied/satisfied” or “angry/calm”). The CFA showed unsuitable fit indices (χ^2/101=2.493, *p*<.001; CFI=.898, TLI=.862, RMSEA=.084). By using Lagrange multipliers as well as applying rules for psychometric quality as stated in section “Data analysis strategy” we excluded three items (one per dimension). The resulting model showed good fit indices (χ^2/62=1.649, *p<.001*; CFI=.966, TLI=.957, RMSEA=.056). The solution has convergent validity (for all factors): AVE_{EoU}=.436, CR_{EoU}=.754; $AVE_{Usefulness}$=.671, $CR_{Usefulness}$=.889; AVE_{fun}=.550, CR_{fun}=.859).

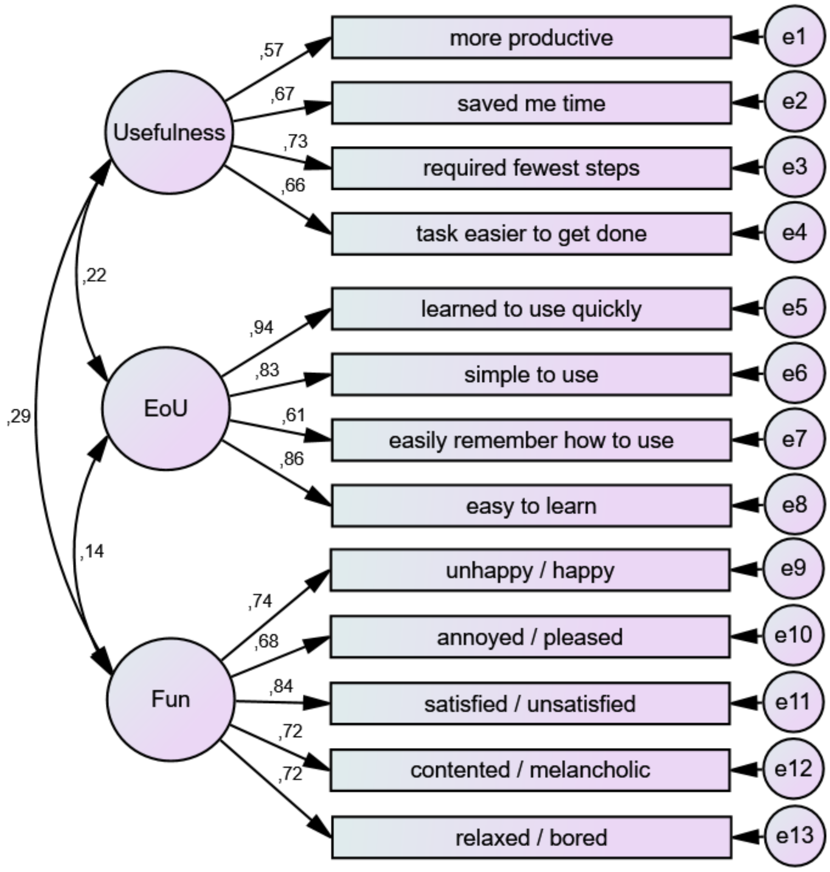

Figure 2.2 – CFA for C-TAM

Trust was measured Using Reid and Levy's scale (2008) that comprehends a single factor (5 items, e.g. "I feel safe in placing my personal information in my smartphone" and "I believe my smartphone has built-in mechanisms to protect users"). The CFA showed invalid fit indices (χ^2/5=12.161, *p*<.001; CFI=.865, TLI=.596, RMSEA=.231). From applying Lagrange multipliers we found a valid four-item solution (χ^2/2=1.448, *p=.235*; CFI=.997, TLI=.992, RMSEA=.046) that also has convergent validity (AVE=.560, CR=.835). Respondents were requested to answer in a 5 point Likert scale from strongly disagree) to 5 (strongly agree).

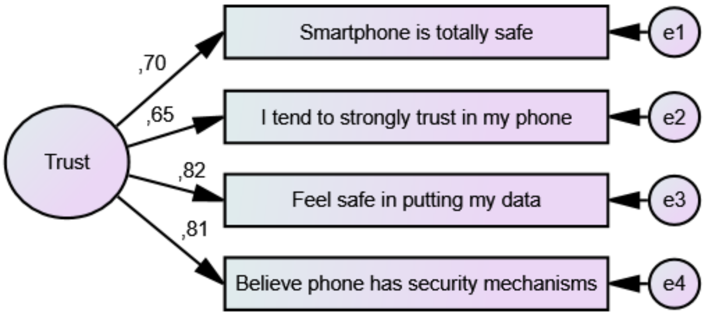
Trust
,70
,65
,82
,81
Smartphone is totally safe
I tend to strongly trust in my phone
Feel safe in putting my data
Believe phone has security mechanisms
e1
e2
e3
e4

Figure 2.3 – CFA for trust in smartphones

Sociodemographic and control variables were included not only to characterize the sample but also as control variables. Namely: gender (dummy coded for 1=”Male” and 2=”Female”), age (coded as continuous variable), education (1=”<9 years schooling”, 2=”9th grade”, 3=”12th grade”, 4=”Degree”, 5=”Master”, 6=”PhD”), civil status (1=”Single”, 2=”Married”, 3=”Divorced”, and 4=”Widowed”). We also used the additional control variables: IT-related occupation (dummy coded for 1=”Yes”, 2=”No”), uses vs not uses smartphone (dummy coded for 1=”Yes”, 2=”No”), time using smartphone (number of years), % of people around using smartphone (free choice 0% to 100%), awareness of AI use in own smartphone (ranging 1=”It incorporates nothing even closer to AI” to 7=”It incorporates a great deal of AI, even more than people think”).

Chapter III – Results

This chapter will show findings concerning the descriptive statistics of the variables involved in this research followed by the bivariate statistics, so to have a global grasp of associations between data.

3.1. Descriptive and bivariate statistics

Table 3.1 shows the mean, standard-deviation and range for the sociodemographics and key variables under study.

	Scale range	Min-max	med	s.d.
1. Age	18 - …	18-69	30.16	11.73
2. Gender	1-2	1-2	70.8%fem	-
3. Education	1-6	-	-	-
4. Marital status	1-4	-	-	-
5. IT_profession	1-2	1-2	79.2% no	-
6. Familiarity	0-100	0-100	69.9%	22.1%
7. Awareness	1-7	1-7	4.98	1.46
8. CTAM_Usefulness	1-5	1-5	3.82	0.73
9. CTAM_EoU	1-5	2.5-5	4.66	0.55
10. CTAM_fun	1-5	1-5	3.407	0.81
11. Trust	1-5	1-5	3.17	0.89
12. BI_money	1-5	1-5	2.65	1.01
13. BI_social	1-5	1.33-5	4.32	0.77
14. BI_health	1-5	1-5	2.14	1.16
15. BI_biometrics	1-5	1-5	1.69	1.24

Table 3.1 – Descriptive statistics

Besides the sociodemographics, already described in the sample characterization, it is worth noting that participants express a degree of familiarity with AI that falls slightly below 70% and they state an average degree of awareness about their smartphone AI above the midpoint of the scale suggesting they believe they are aware of its presence.

The set of variables that compose C-TAM (usefulness, ease-of-use, and fun) vary substantially although their mean is always above the midpoint of the scale. Fun is the most highly rated (M=5.97) although the most dispersed (s.d.=1.53) which suggests more heterogeneity between participants which also evidences the added value in considering the hedonic dimension in this sort of studies as compared with using the original TAM model. The second highly rated dimension is ease-of-use (M=4.66, sd=0.55) followed by usefulness (M=3.83, sd=0.73). It is also interesting that ease-of-use scale was never chosen (on the average) below 2 which strongly suggests this population feel at ease with this sort of gadget.

Being a central variable in this study, trust is of special importance. It is interesting that it was averagely rated as 3.17 (sd=0.89), slightly above the midpoint ($t_{(191)}$ = 2.619, p<.01, CI95 [.041; .294]) and therefore, although we can state it is higher than "Neither agree nor disagree" it is not as high as one could expect in regular user of AI embedding smartphones.

Behavioral intention varies according with the specific category of the application under consideration. It reaches is lowest for biometrics use (M=1.69, sd=1.24) and its highest mean value for social apps use (M=4.32, sd=0.77). In between one finds the intention to use the smartphone for money related applications (M=2.65, sd=1.01) and health related application (M=2.14, sd=1.16). Overall the means make the use of smartphones for social related applications the most wide and popular behavioral intention (matching the popularity of social networks). The availability of the technology may also explain partially results as biometrics is not a built-in feature is the majority smartphones models.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1. Age	1													
2. Gender	-.029	1												
3. Education	-.169*	.077	1											
4. Marital status	.692**	.047	-.232**	1										
5. IT_profession	.047	.342**	.080	.024	1									
6. Familiarity	-.304**	-.194**	.174*	-.326**	-.236**	1								
7. Awareness	-.118	.002	.251**	-.170*	-.099	.123	1							
8. CTAM_Usefulness	-.037	-.032	.240**	-.035	-.163*	.175*	.094	1						
9. CTAM_EoU	-.487**	.107	-.021	-.233**	-.109	.362**	.118	.190**	1					
10. CTAM_fun	-.084	.023	.118	-.089	-.123	.046	.106	.244**	.103	1				
11. Trust	-.258**	.057	.109	-.062	-.101	.166*	.068	.322**	.334**	.222**	1			
12. BI_money	-.314**	-.142	.099	-.185*	-.197**	.251**	.235**	.217**	.274**	.117	.372**	1		
13. BI_social	-.415**	.128	.219**	-.312**	-.007	.219**	.217**	.233**	.299**	.091	.434**	.422**	1	
14. BI_health	-.202**	-.025	.006	-.111	-.107	.129	.123	.179*	.180*	.076	.327**	.338**	.277**	1
15. BI_biometrics	-.126	-.092	.005	-.027	-.084	.107	.073	.135	.051	.155*	.328**	.205**	.101	.347**

Table 3.2 – Bivariate statistics

Overall, sociodemographics show expected patterns of association as older participants tend to report being less educated, and less familiar with AI. The sample, as stated, is largely feminine and it is interesting to find that despite this, male sample is more closely associated with being an IT professional, which matches the overall market gender profile in IT professions. Education showed positive association with both familiarity with AI use in smartphones as well as being aware of its presence in the personal smartphone. Likewise, those participants that stated they worked as IT professionals are reporting higher levels of familiarity but there is no relation between being an IT professional and the level of awareness participants reported. Also, analyzing the associations between sociodemographic variables and the key variables included in the research model, it is evident that age is largely associated with several. Older individuals are less prone to rate high ease-of-use (older individuals find smartphones less easy to use), tend to trust less in their smartphones, and tend to use less the social-related, money-related and health-related applications. Expectable, familiarity is positively associated with usefulness, ease-of-use, intention to use money-related applications, and social-related applications. The level of awareness also tends to co-occur with higher intentions to use these two sorts of applications. It is worth noticing that trust is not related with any sociodemographic variables, to the exception of age.

C-TAM variables also show an expectable pattern of association with trust as all the three variables show a positive correlation with trust. Likewise, in most cases, C-TAM variables are positively associated with intention to use (to the exception of biometrics that only shows a significant association (with fun) albeit of a very weak magnitude (r=.155, p<.05). Trust is also more associated with the behavioral intention to use all four sorts of applications.

3.2. Hypotheses testing

The fully integrated analytical model was designed as a set of structural equations that included all latent variables as well as hypothesized relationships between them. The model showed acceptable fit (χ^2/df=1.409, p<.001; CFI=.938, TLI=.928, RMSEA=.044, SRMR=.070) which means the coefficients are interpretable. Table 3.3 summarizes findings for direct and indirect effects for the many paths included in the structural model. Association coefficients as well as the respective bootstrapped lower and upper bounds for 95% confidence intervals are shown between brackets.

Path	Total effect		Direct effect		Indirect effect		Type of mediation
	b	CI95 LB; UB	b	CI95 LB; UP	b	CI95 LB; UP	
EoU -> Usefullness -> Trust	.399	(.205;.639)	.311	(.123;.534)	.088	(.016;.215)	Partial
EoU -> Fun -> Trust	.413	(.209;.669)	.380	(.178; .625)	.033	(.001;.117)	Partial
Usefulness -> Trust -> Biometrics	.288	(-.052;.559)	.032	(-.400; .406)	.256	(.114;.553)	Total
Usefulness -> Trust -> Money	.324	(.098;.649)	.115	(-.150; .433)	.209	(.093;.439)	Total
Usefulness -> Trust -> Social	.324	(.064;.712)	.147	(-.145; .472)	.177	(.079;.388)	Total
Usefulness -> Trust -> Health	.349	(.031;.687)	.101	(-.342; .468)	.247	(.103;.517)	Total
Fun -> Trust -> Biometrics	.155	(.037; .313)	.085	(-.050;.229)	.070	(.014;.190)	Total
Fun -> Trust -> Money	.069	(-.046; .203)	.004	(-.137; .139)	.064	(.011;.174)	Total
Fun -> Trust -> Social	.025	(-.055; .128)	.053	(-.133; .053)	.157	(.014;.157)	Total
Fun -> Trust -> Health	.067	(-.068; .206)	-.010	(-.192; .137)	.076	(.013;.204)	Total
EoU -> Useful -> Trust -> Biom.	-.016	(-.297;.190)	-.266	(-.629; -.011)	.250	(.109;.494)	Partial
EoU -> Useful -> Trust -> Money	.266	(.057;.492)	.081	(-.121;.283)	.186	(.079;.354)	Total
EoU -> Useful -> Trust -> Social	.206	(-.060;.553)	.034	(-.238;.338)	.172	(.084;.331)	Total
EoU -> Useful -> Trust -> Health	.200	(-.019;.411)	-.029	(-.298;.213)	.229	(.095;.452)	Total
EoU -> Fun -> Trust -> Biom.	-.006	(-.293; .205)	-.265	(-.629; -.013)	.259	(.118; .504)	Partial
EoU -> Fun -> Trust -> Money	.272	(.063; .508)	.093	(-.102; .304)	.179	(.074; .350)	Total
EoU -> Fun -> Trust -> Social	.206	(-.061; .560)	.044	(-.220; .351)	.161	(.073; .312)	Total
EoU -> Fun -> Trust -> Health	.204	(-.019; .422)	-.026	(-.295; .224)	.230	(.093; .444)	Total

Table 3.3 – coefficient and CI95 for mediational paths

Findings show a meaningful direct effect of .311CI95 [.123;.534] between easy-of-use and trust as well as a meaningful indirect effect of .088 via usefulness CI95 [.016;.215] which corresponds to a partial mediation, **thus supporting hypothesis 1a**, indicating that usefulness partially mediates the positive relationship between easy-of-use and trust. Likewise, findings show a meaningful direct effect of .380 CI95 [.178; .625] between easy-of-use and trust as well as a meaningful indirect effect of .033 via fun CI95 [.001;.117] which corresponds to a partial mediation, **thus supporting hypothesis 1b**, indicating that Fun partially mediates the positive relationship between easy-of-use and trust.

As regards the possible mediating role trust plays between CTAM components and behavioral intentions to use smartphone apps, findings show all cases have a meaningful indirect effect, namely .256 CI95 [.114;.553] for biometrics; .209 CI95 [.093;.439] for money-related; .177 CI95 [.079;.388] for social-related; and .247 CI95 [.103;.517] for health-related apps. As no direct meaningful effect was found between usefulness and any of the behavioral intention variables, findings correspond to total mediations, **thus supporting hypothesis 2a**. This indicates trust is a total mediator between usefulness and behavioral intentions. The counterpart for the hedonic path via fun also shows, for all cases, meaningful indirect effects, namely .070 CI95 [.014;.190] for biometrics; .064 CI95 [.011;.174] for money-related; .157 CI95 [.014;.157] for social-related; and .076 CI95 [.013;.204] for health-related apps. As no direct meaningful effect was found between usefulness and any of the behavioral intention variables, findings correspond to total mediations, **thus supporting hypothesis 2b**. This indicates trust is also a total mediator between Fun and behavioral intentions.

As regards the **three-path sequential mediation via usefulness**, findings show a meaningful direct negative effect between easy-of-use and **biometrics** (b=-.266 CI95 [-.629; -.011] as well as a meaningful indirect effect via usefulness followed by trust (b=.250 CI95 [.109;.494] which corresponds to a partial mediation. Although the sequential mediation occurs, this does not support hypothesis **3a.1** due to the negative valence of the association. When taking into consideration the same path leading to intention to use **money-related apps**, findings show a meaningful positive indirect effect (b=.186 CI95 [.079;.354] with a non-meaningful direct effect, thus corresponding to a total mediation. This supports hypothesis **3a.2**. For **social-related and health-related** apps, findings are similar with a b=.172 CI95 [.084;.331] and b=.229 CI95 [.095;.452] respectively. This matches a total mediation for both cases, which supports hypotheses **3a.3** and **3a.4**.

As regards the three-path sequential mediation via fun, findings show a meaningful direct negative effect between easy-of-use and **biometrics** (b=-.265 CI95 [-.629; -.013] as well as a meaningful indirect effect via Fun followed by trust (b=.259 CI95 [.118; .504] which corresponds to a partial mediation. This does not support hypothesis **3b.1** due to the negative valence of the association. When taking into consideration the same path leading to intention to use **money-**

related apps, findings show a meaningful positive indirect effect (b=.179 CI95 [.074; .350] with a non-meaningful direct effect, thus corresponding to a total mediation. This supports hypothesis **3b.2**. For **social-related and health-related** apps, findings are similar with a b=.161 CI95 [.073; .312] and b=.230 CI95 [.093; .444] respectively. This matches a total mediation for both cases which supports hypotheses **3a.3** and **3a.4**.

To test for common method bias, as advisable taking into consideration the subjective nature of variables simultaneously with a single source (Podsakoff et al., 2003) we conducted a single latent variable linking directly to each observable item of all constructs involved in the model to the exception of the control variables. Results showed paths with non-significant (p>.01) standardized .26 coefficients which encourage us to rule out common method bias.

Overall, both the cognitive path (via usefulness) and the hedonic path (via fun) gained general empirical support.

Chapter IV – Discussion and Conclusion

This study explored an integrated model that brings together C-TAM (Bruner & Kumar, 2003) and an important psychosocial factor: trust. As stated, trust plays a fundamental role in understanding behavioral intentions and actual behavior (Gefen, Karahanna, & Straub, 2003) in the sense that it is a requirement to willingly use technology where it is available but not imposed. By adopting C-TAM this study also incorporates the cognitive and hedonic channels which are more in line with a consumer point of view (Bruner & Kumar, 2003).

The first finding worth discussion is the reported degree of familiarity with AI in smartphones. The 70% average is expected even from a non-technical population as AI reaches pop culture via movies (Siau & Wang, 2018) and is increasingly showed as an added value by the smartphone producers themselves. Also, there is a tendency to positively bias own knowledge about desirable topics as a way not to show oneself ignorance (Dunning, Heath & Suls, 2004). The fact that IT professionals do not differ from non-IT professionals in regards to the self-reported degree of awareness about the use of AI in their personal smartphones is highly suggestive of an overly optimistic self-representation of the common individual concerning their knowledge about technical domains. As AI entered the fashion like buzzwords, nonprofessional individuals are led to believe that hearing about is the same and knowing about. This could also be explained by the reported ease-of-use of interfaces, disregarding the complex systems behind them, leading users to believe the simplicity they experience in the interface is matched by its internal technical systems. It is obviously probable that individuals have an idea that they know about AI but do not actually understand the mechanics of the underlying algorithms.

Hypotheses testing are overly suggesting the proposed model is sound. The first and second hypotheses are subsidiary of the third one which is the most comprehensive being, thus, the one that adds more to the discussion and theory building. Indeed, the third hypothesis subdivides into four sub-hypotheses, one per each type of behavioral intention.

The total mediations found for money, social and health-related apps clearly show the central role trust plays in linking technological features (easy-of-use) via both a cognitive path (usefulness) and an affective path (fun) towards intending to actually use smartphone apps which is in line with Hind et al. (2018). Without it, it is not possible to explain individuals' intention to use them. In the special case of biometrics, findings are somewhat surprising in the sense that although there is a mediation in play (partial) the valence of the relationship is negative, thus counterintuitively suggesting that the more individuals find it easy to use the smartphone, the less probable it is for them to intend to use biometric features. This can be interpreted as an indication that biometrics usage is considered as a means to facilitate the use of the smartphone (such as block or unblock security features or access to the main screen) but, judging from the psychometrics of this variable we think this may be a product of measurement error. We believe so because it is the only component to show a non-significant correlation with the other three (social, health, money) besides being measured only with two items. An important indication is that it may not be sufficiently common usage to lead consumers to think about it (as suggested by the modest mean of 1.69 and sd=1.24 in a 1-5 scale).

Support given to H1a and H1b shows C-TAM operates as a packed set of variables that relate all with trust. Due to the consistent total mediations found for trust between C-TAM variables and apps intended usage as stated under H2, it is clear that trust is a necessary condition in this equation. Its importance cannot be understated in situations where usage is voluntary (Gefen et al., 2003). In the full sequential equation predicted in H3, only the paths leading to biometrics fail to match a total mediation. This is arguably an exception to the rule due to the psychometric issues concerning biometrics that we have already pointed out. Giving support to the original TAM (Davis, 1986) and revised C-TAM (Bruner & Kumar, 2003) ease-of-use can be taken as a facilitator of the perception of usefulness as well as fun. Extending its application to smartphones, with a focus on AI, findings pertaining H3 also highlight the role trust plays as a necessary condition to bridge technology acceptance with voluntary app usage. This is especially interesting because AI might be taken as familiar, but it is for the large majority of consumers, a black-box and thus we are operating at the level of beliefs and attitudes. This reinforces the fortunate choice of trust in conducting this empirical study.

Other choices have not been as fortunate and may hamper the robustness of findings. Such was the case of the sample size which, albeit being sufficiently large to conduct data analysis, it is not comfortable when conducting a SEM with so many parameters. We believe the option to bootstrapping may cushion this but it is not ascertainable with the data we have. The sample could also be more gender balanced as the vast majority of participants were female. This is probably due to the activation of snow-ball sampling which involved colleagues from courses that have an over representation of women. Future studies may benefit from ensuring a more gender balanced samples. Despite this, gender effects were controlled for but we still, are left with the impression that the overall medians may have reflected this (Van Deursen, Bolle, Hegner & Kommers, 2015).

As in all mediation models, the collection of data from the same source, especially data of a subjective or perceptive nature, is prone to common method / source bias (Podsakoff et al., 2003). As shown, findings rule out such common variance although we would be much more comfortable with at least a two-wave data collection procedure, that is not so compatible with the time frame available to complete a master thesis. Other limitation we felt was due to the hardly existing psychological literature targeting AI enabled gadgets. The existing body of knowledge about trust is mostly produced under the assumption that it pertains interpersonal relationship. However, the technological breakthroughs that simulate human entities but operate as a replacement of relationships (e.g. Siri, Alexa, Cortana, chatbots) being able to interact using natural language and designed to mimic human emotions, opens way to a novel domain in the research of psychosociology by targeting this “as if” layer in human – AI interaction.

Future studies may greatly extend these findings by targeting specific samples, e.g. that use a certain smartphone brand with enabled AI functions, also crossing those with advertised features. This would allow for the control of brand-specific effects.

Bibliography

Abdalla, I. (2007). Evaluating effectiveness of e-blackboard system using TAM framework: A structural analysis approach. *AACE Journal, 15*(3), 279-287.

Abubaker, H., Shamsuddin, S. M., & Ali, A. (2018). Analytics on malicious android applications. *International Journal of Advances in Soft Computing & Its Applications*, *10*(1), 106-118.

Adams, B. D., Bruyn, L. E., Houde, S., Angelopoulos, P., Iwasa-Madge, K., & McCann, C. (2003). Trust in automated systems. *Ministry of National Defence*.

André, E., Baker, R., Hu, X., Rodrigo, M. M. & Boulay, B. (2017). Artificial intelligence in education: 18th International Conference, AIED 2017, Wuhan, China, June 28 – July 1, 2017, Proceedings (Vol. 10331). Springer International Publishing AG.

Anwar, A. & Hassan, S. I. (2017). Applying artificial intelligence techniques to prevent cyber assaults. International Journal of Computational Intelligence Research, 13(5), 883-889.

Atkinson, R. D. (2016). "It's going to kill us!" and other myths about the future of artificial intelligence. Information Technology & Innovation Foundation. Retrieved from http://www2.itif.org/2016-myths-machine-learning.pdf

Baier, A. (1986). Trust and antitrust. *ethics*, *96*(2), 231-260.

Bruner II, G. C., & Kumar, A. (2005). Explaining consumer acceptance of handheld Internet devices. *Journal of business research*, *58*(5), 553-558.

Childers, T. L., Carr, C. L., Peck, J., & Carson, S. (2001). Hedonic and utilitarian motivations for online retail shopping behavior. *Journal of retailing*, *77*(4), 511-535.

Copeland, J. (1993). Artificial intelligence: A philosophical introduction. John WileyBlackwell.

Couch, L. L., & Jones, W. H. (1997). *Measuring Levels of Trust. Journal of Research in Personality, 31(3), 319–336.*

Dabholkar, P. A., & Bagozzi, R. P. (2002). An attitudinal model of technology-based self-service: moderating effects of consumer traits and situational factors. *Journal of the academy of marketing science*, *30*(3), 184-201.

Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* (Doctoral dissertation, Massachusetts Institute of Technology).

Deutsch, M. (1958). Trust and suspicion. Conflict resolution, 2, 265–279.

Dunning, D., Heath, C., & Suls, J. M. (2004). Flawed self-assessment: Implications for health, education, and the workplace. *Psychological science in the public interest*, *5*(3), 69-106.

Egele, M., Kruegel, C., Kirda, E., & Vigna, G. (2011, February). PiOS: Detecting Privacy Leaks in iOS Applications. In *NDSS* (pp. 177-183).

Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B. G., Cox, L. P., ... & Sheth, A. N. (2014). TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. *ACM Transactions on Computer Systems (TOCS)*, *32*(2), 5.

Ertel, W. (2017). *Introduction to artificial intelligence* (2nd ed.). Cham, Switzerland: Springer International Publishing AG.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. *MIS quarterly*, *27*(1), 51-90.

Gips, J. (1979). Artificial Intelligence. *Environment and Planning B, 6*, 353-364.

Hayes, A. F. (2017). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. Guilford Publications.

Hengstler, M., Enkel, E., & Duelli, S. (2016). Applied artificial intelligence and trust—The case of autonomous vehicles and medical assistance devices. *Technological Forecasting and Social Change*, *105*, 105-120.

Hillman, D. J. (1985). Artificial Intelligence. *Human Factors, 27*(1), 21-31.

Hind, M., Mehta, S., Mojsilovic, A., Nair, R., Ramamurthy, K. N., Olteanu, A., & Varshney, K. R. (2018). Increasing Trust in AI Services through Supplier's Declarations of Conformity. *arXiv preprint arXiv:1808.07261*.

Holmes, J. G. (1991). Trust and the appraisal process in close relationships.

Jeon, W., Kim, J., Lee, Y., & Won, D. (2011). A Practical Analysis of Smartphone Security. *Lecture Notes in Computer Science Human Interface and the Management of Information. Interacting with Information,*311-320. doi:10.1007/978-3-642-21793-7_35

Jones, K. (1996). Trust as an affective attitude. *Ethics*, *107*(1), 4-25.

Kevin Mahaffey, John Hering: App Attack: Surviving the Explosive Growth of Mobile Apps (2010)

Lacohee, H. , Wakeford, N. & Pearson, I. (2003). A social history of the mobile telephone with a view of its future. *BT Technology Journal, 21*(3), 203-211

Larzelere, R. E., & Huston, T. L. (1980). The dyadic trust scale: Toward understanding interpersonal trust in close relationships. *Journal of Marriage and the Family*, 595-604.

Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human factors*, *46*(1), 50-80.

Lewicki, R. J., Tomlinson, E. C., & Gillespie, N. (2006). Models of interpersonal trust development: Theoretical approaches, empirical evidence, and future directions. *Journal of management*, *32*(6), 991-1022.

Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. *Social forces*, *63*(4), 967-985.

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems*, *17*(1), 39-71.

Lisetti, C. L., & Schiano, D. J. (2000). Automatic facial expression interpretation: Where human-computer interaction, artificial intelligence and cognitive science intersect. *Pragmatics & Cognition, 8*(1), 185-235.

Luger, G. F. (2009). *Artificial intelligence: Structures and strategies for complex problem solving* (6th Edition). Boston, United States of America: Pearson Education, Inc.

Luo, X. (2002). Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management*, *31*(2), 111-118.

Makridakis, S. (2017). The forthcoming Artificial Intelligence (AI) revolution: Its impact on society and firms. *Futures*, *90*, 46-60.

McAllister, D. J. (1995). Affect-and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of management journal*, *38*(1), 24-59.

McKnight, D. H., & Chervany, N. L. (2000). What is trust? A conceptual analysis and an interdisciplinary model. *AMCIS 2000 Proceedings*, 382.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research*, *13*(3), 334-359.

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management review*, *23*(3), 473-490.

Muir, B. M. (1994). Trust in automation: Part I. Theoretical issues in the study of trust and human intervention in automated systems. *Ergonomics*, *37*(11), 1905-1922.

Mulliner, C.R.: Security of Smart Phone, Master's Thesis of University of California (June 2006)

Nilsson, N. J. (2014). Principles of artificial intelligence. Morgan Kaufmann Publishers.

O'Dell, D. G., & Sulastri, T. (2019). The Impact of Using the Internet for Learning for Students with Technology Acceptance Model (TAM). *International Journal of Environment, Engineering & Education, 1*(2), 46-52.

Oleson, K. E., Billings, D. R., Kocsis, V., Chen, J. Y., & Hancock, P. A. (2011, February). Antecedents of trust in human-robot collaborations. In *2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)* (pp. 175-178). IEEE.

Paluch, S. & Wünderlich, N.V. (2016). Contrasting risk perceptions of technology-based service innovations in inter-organizational settings. *Journal of Business Research, 69*, 2424–2431.

Pando-Garcia, J., Periañez-Cañadillas, I., & Charterina, J. (2016). Business simulation games with and without supervision: An analysis based on the TAM model. *Journal of Business Research, 69*(5), 1731-1736.

Pannu, A. (2015). Artificial intelligence and its application in different areas. *International Journal of Engineering and Innovative Technology, 4*(10), 79-84.

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information systems research*, *15*(1), 37-59.

Punyatoya, P. (2019). Effects of cognitive and affective trust on online customer behavior. *Marketing Intelligence & Planning*, *37*(1), 80-96.

Rempel, J. K., Holmes, J. G., & Zanna, M. P. (1985). Trust in close relationships. *Journal of personality and social psychology*, *49*(1), 95-112.

Robinson, H., MacDonald, B. & Broadbent, E. (2014). The role of healthcare robots for older people at home: A review. *International Journal of Social Robotics, 6*(4), 575-591.

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality, 35*, 651–665.

Rotter, J. B. (1971). Generalized expectancies for interpersonal trust. *American psychologist*, *26*(5), 443.

Russel, S. & Norvig, P. (1995). *Artificial intelligence: A modern approach*. Englewood Cliffs, New Jersey: Prentice-Hall, Inc.

Sánchez, R. A., & Hueros, A. D. (2010). Motivational factors that influence the acceptance of Moodle using TAM. *Computers in human behavior, 26*(6), 1632-1640.

Shapiro, S. P. (1987). The social control of impersonal trust. *American journal of Sociology*, *93*(3), 623-658.

Siau, K., & Wang, W. (2018). Building trust in artificial intelligence, machine learning, and robotics. *Cutter Business Technology Journal*, *31*(2), 47-53.

Sitkin, S. B. (1995). On the positive effects of legalization on trust. *Research on negotiation in organizations*, *5*, 185-218.

Talal, M., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Alsalem, M. A., Albahri, A. S., ... & Alaa, M. (2019). Comprehensive review and analysis of anti-malware apps for smartphones. *Telecommunication Systems*, 1-53.

Van Deursen, A. J., Bolle, C. L., Hegner, S. M., & Kommers, P. A. (2015). Modeling habitual and addictive smartphone behavior: The role of smartphone usage types, emotional intelligence, social stress, self-regulation, age, and gender. *Computers in human behavior*, *45*, 411-420.

Wang, L., Rau, P. L. P., Evers, V., Robinson, B. K., & Hinds, P. (2010, March). When in Rome: the role of culture & context in adherence to robot recommendations. In *Proceedings of the 5th ACM/IEEE international conference on Human-robot interaction* (pp. 359-366). IEEE Press.

Xiao, Q. (2007). Technology review-biometrics-technology, application, challenge, and computational intelligence solutions. *IEEE Computational Intelligence Magazine*, *2*(2), 5-25.

Yu, F. (2012). Mobile/Smart Phone Use in Higher Education. In M. Rao (Ed.), Southwest Decision Science Institute Conference (pp. 831–839). Houston, Texas, USA: Decision Sciences Institute. Retrieved from http://www.swdsi.org/swdsi2012/proceedings_2012/papers/Papers/PA144.pdf

Zhou, Y., Zhang, X., Jiang, X., & Freeh, V. W. (2011, June). Taming information-stealing smartphone applications (on android). In *International conference on Trust and trustworthy computing* (pp. 93-107). Springer, Berlin, Heidelberg.

Zucker, L.G., 1986. Production of trust: Institutional sources of economic structure. In: Staw, B.M., Cummings, L.L. (Eds.), *Research in Organizational Behavior*. JAI Press, Greenwich, CT, pp. 840–1920.