

Trust-based framework for Information Sharing in Health care

by

Saghar Behrooz

A thesis submitted in partial fulfillment
of the requirements for the degree of

Masters of Science

in

Computer Science

University of Ontario Institute of Technology

Supervisor: Dr. Stephen Marsh

October 2016

Copyright © Saghar Behrooz, 2016

Abstract

The use of information systems in the health care area specifically in Mobile health care, can result in delivering high quality and efficient patient care. At the same time, using electronic systems for sharing information contributes to some challenges regarding privacy and access control. Despite the importance of this issue, there is a lack of frameworks in this area. In this research, we propose a trust-based model for information sharing between mobile health care applications. This model consists of two parts, the first part calculates the needed amount of trust for sharing a specific part of information for each user, and the second part calculates the (contextual) current existing amount of trust. A decision about sharing information would be made based on a comparison between the components. Different scenarios of information sharing are provided. Using mathematical analysis, we illustrate how the model works in these scenarios. To provide the ability of comparison between current models and the proposed model, an iOS application as a representative of the model is designed and implemented. To examine the model, a within subject user study is conducted. In this study users interacted with both Apple health interface and the trust reasoning application. Results, highlighted that the proposed application has an impact on the user's perception and awareness of privacy. The proposed model was chosen as the preferred model by users.

Keywords: trust, trust management, mobile health care, information security, user

study, trust-based mobile application

Acknowledgements

I would like to express my sincere gratitude to my advisor and mentor Dr. Stephen Marsh for his support and guidance throughout my research. His knowledge and passion were a source of motivation. His invaluable guidance was instrumental towards the success of this project and his continuous support and mentorship made me a better person.

I would like to thank my family. My parents have always been encouraging and supportive of me. Last, but certainly not least, I thank my sisters, Sara and Samira, without their limitless support none of this would have been possible.

Publications

Contribution of this research is published in:

- Behrooz, Saghar, and Stephen Marsh. “A Trust-Based Framework for Information Sharing Between Mobile Health Care Applications.” IFIP International Conference on Trust Management. Springer International Publishing, 2016.
- “Serene Risc” Poster session, Fall 2016

Contents

Abstract	i
Acknowledgements	iii
Publications	iv
Contents	v
List of Figures	ix
List of Tables	xi
1 Introduction	1
1.1 Motivation	2
1.2 Objectives	3
1.3 Thesis Outline	5
2 Background	6
2.1 Health Information Management	7
2.1.1 Mobile Health	7
2.1.2 Privacy	8
2.2 Trust Models in Health care Information Systems	9

2.3	Trust Management	11
2.3.1	Definition of Trust	11
2.3.2	Computing Trust	13
2.3.3	Trust, Privacy and Security	16
2.3.4	Comfort	17
2.4	Conclusions	17
3	Apple’s HealthKit Framework	19
3.1	Overview	19
3.2	HealthKit Design	20
3.2.1	HealthKit Store	21
3.3	Privacy in HealthKit	23
3.4	Privacy in mHealth	23
3.5	Conclusion	24
4	The B-Trust Model	25
4.1	Calculation of the Trust Value for Specific Types of Information	27
4.2	The Personal Perspective	29
4.2.1	Sensitivity of Information	29
4.2.2	T_d : Delay Time	35
4.3	Context Perspective	36
4.3.1	Default trust to each category and purpose	37
4.3.2	Application Rating (public social)	38
4.3.3	Social network friends	38
4.3.4	Installer of the Application:	39
4.3.5	Estimation of the Threshold	40
4.4	Conclusion	40

5	Theoretical Examples	42
5.1	Various Agents	42
5.2	Pool of Applications	43
5.3	Various Situations	45
5.3.1	Scenario 1– Installing Random Applications	46
5.3.2	Scenario 2 – Various Rated Applications	46
5.3.3	Scenario 3– Installing Applications Suggested by Trusted Persons	46
5.3.4	Scenario 4- Share Everything	47
5.4	Mathematical Analysis	47
5.5	Conclusion	63
6	Experiment: Investigating the Impact of the Trust-reasoning In-	
	terface on Users	65
6.1	Use of User Study as an Evaluation Method	66
6.2	Evaluation Goals	66
6.3	Application Design and Developement	67
6.3.1	User Interface	67
6.3.2	User Interface Design Criteria	68
6.4	Methodology	72
6.4.1	Experimental Environment	72
6.4.2	Participants	73
6.4.3	Procedure	73
6.4.4	Questionnaire Design	76
6.4.5	Results	76
6.5	Discussion	78
6.6	Limitations	84

6.7 Conclusion	84
7 Conclusions	86
7.1 Research Contributions	86
7.2 Future Work	87
7.3 Conclusion	88
Appendix	90
Bibliography	95

List of Figures

3.1	Example of Apple HealthKit interface	22
4.1	Architecture of B-trust model	26
6.1	A screen shot of vital signs information slider	69
6.2	The “category of information” input screen	70
6.3	The “purpose of information” input screen	71
6.4	The delay time input screen	72
6.5	Fourth screen- Results	73
6.6	Example of Apple HealthKit interface	75
6.7	Description of ANOVA- App 1: Trust-reasoning, App 2: Apple Health- Figure illustrates that the score mean of all answers for Trust reason- ing application is higher than Apple application. Score of answers to question 3 has the lowest mean.	78
6.8	Description of MEAN Analysis - App 1: Trust-reasoning, App 2: Apple Health	80
6.9	Description MEAN Analysis - App 1 = Trust reasoning, App 2= Apple Health	83
7.1	Appendix 1- Invitation Letter	91

7.2	Appendix 2- Apple Questionnaire	92
7.3	Appendix 3- BTHealth Application Questionnaire	93
7.4	Appendix 3- BTHealth Application Questionnaire- Page 2	94

List of Tables

4.1	Explanation of Notations	28
4.3	Information Categories	30
5.1	Trust Values Assigned by Tracy	48
5.2	Trust Values Assigned by Steve	51
5.3	Trust Values Assigned by Bob	54
5.4	Trust Values Assigned by Julia	58
6.1	Explanation of icons were used in the interface	68
6.2	Likert scale answers	77
6.4	Correlation (Pearson's R) of Questions	79

Chapter 1

Introduction

Development of technology has enabled mobile devices as appropriate tools for facilitating health care of various types, in what is known as mHealth. mHealth provides the opportunity to store and share the health information of a patient in their personal devices in order to enhance and deliver more efficient and personal services, from fitness advice to more physician-oriented tools. However, security of the information, in addition to access control measures, are among the controversial issues in this area [53]. Health care applications collect and share various types of information regarding physical activities and the lifestyles of users in addition to their medical and physiological information [48]. Collection of broader sensitive information raises privacy issues that should be better managed [13].

To address this, in this thesis, we are proposing a trust model which is used by the owners of the information to help them make decisions about sharing their information or part of it with a specific application. To formalize the trust value

for each purpose of information, there are two components of a trust model which must be calculated. The first component of the model calculates the amount of trust which each person needs for sharing a specific part of the information. The second component of the model calculates the amount of trust already extant between a device and the application which is asking for the information. In the end, calculated trust values of each component would be compared and decision would be made.

1.1 Motivation

Use of health information which is collected through mobile devices can improve quality of care [78]. However, privacy and security measures are not able to address the concerns regarding these issues. According to the National Committee for Vital and Health Statistics (NCVHS), health information privacy is “An individual’s right to control the acquisition, uses, or disclosures of his or her identifiable health data. Confidentiality, which is closely related, refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate. Security is altogether different. It refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure” [8].

In 2015 more than 24,000 health mobile application existed for iOS and Android. The majority of applications (95.63%) pose potential damage regarding security and privacy [25]. Recently, both Google and Apple announced new platforms for health

apps such as HealthKit [2], ResearchKit and GoogleKit [4], which provide the possibility of information sharing between health care applications in one place.

We consider Apple HealthKit as an example. Currently, each application is individually responsible for obtaining the trust of the user in order to get access to their health information. Health information has been divided into different categories. However, once the user shares their information, they have no further control over it. There has been extensive research in this area, however, this research has been focused on making policies or implementing traditional mechanisms such as data encryption. Considering the importance of this information, in addition to usual privacy measurements, other considerations in design such as privacy in design, and need to be met.

1.2 Objectives

The first part of the thesis investigates information systems in the health care area, specifically in mobile healthcare and its privacy issues. Aiming to solve these issues, B-trust model is presented. Development of an interface based the presented model in Chapter 4 is required in order to investigate the usability of the model. In order to investigate how the mobile users experience and understand privacy while they are using health information applications, and whether the proposed interface can result in privacy improvements in systems or not, as well as improving privacy awareness in users, a human study has been conducted. Moreover, the study aimed to answer the

following research questions:

- **RQ1:** How do mobile users experience privacy while they are using health information-based applications?

H0: The *Apple Health application* has a positive impact on the user's perception about privacy.

H1: The *Trust-reasoning application* has a positive impact on the user's perception about privacy.

- **RQ3:** Does the proposed model and interface result in privacy awareness?

H0: The *Apple Health application* has a positive impact on the user's awareness about the privacy of their health information.

H1: The *Trust-reasoning application* has a positive impact on the user's awareness about the privacy of their health information.

- **RQ2:** Does our proposed interface help bring privacy ?

H0: The *Apple Health application* has a positive impact on the user's confidence level for collection and share of their health data by their smart phone.

H1: The *Trust-reasoning application* has a positive impact on the user's confidence level for collection and share of their health data by their smart phone.

1.3 Thesis Outline

This thesis is organized as follows. Chapter 2 provides the basic theoretical background, where some preliminaries on Health Information Systems and mobile health-care are presented. It continues with an overview of trust models and use of them in health information systems. After describing Apple's HealthKit framework in Chapter 3, Chapter 4 presents some notations and definitions which are used in the model, alongside the model itself. The model is evaluated through theoretical analysis in 5. In Chapter 6 the design criteria and development method of the iOS application is presented. This chapter also presents a user study. This user study illustrates the differences between the trust-based model interface and the current in use interface. We conclude with future work in chapter 7.

Chapter 2

Background

The advent of communication, wireless and mobile devices has revolutionized the process of information sharing and storing. With approximately 5 billion users of smartphones, there is a great opportunity for mobile devices to be part of health care services [44]. At the same time, use of mobile devices in the healthcare area can improve diagnosis and treatment guidelines, patient information and administrative efficiency [76]. In this regard, information sharing in health care has a great importance due to the sensitivity of the information in this field. This thesis looks at current privacy policies and systems for health information management, and main strengths and problems with these systems.

2.1 Health Information Management

Systems that use data processing, information and knowledge in order to deliver high quality and efficient patient care in a health care environment are called Health Information Systems [40]. During the last decades, there has been an enormous movement towards computer-based systems from paper-based systems in health care environments [43]. Computer based systems provided the possibility of patient centric systems instead of location based ones [14]. Furthermore, the targeted users of these systems have changed as well. At the beginning, computer-based systems used to target only health care professionals, but as time passed, they also involved patients and their relatives [39]. Developments in these systems over the last few years, provide the possibility of the use of data for care planning and clinical research as well as for patient care purposes [39]. Moreover, continuous health status monitoring using wearable devices such as sensors and watches advances the state of the art for personal health care [52]. Expansions in the use of data and health information in parallel with advancements in technology contributed to the development of different architectures and information systems in this field, including mobile healthcare.

2.1.1 Mobile Health

Mobile health care, m-health, is the use of mobile devices in the health care area in order to improve the quality of care [78]. Special characteristics of mobile devices make them an excellent choice for this purpose, including mobility, the ability to

seamlessly access information and their ubiquity [78]. Employing technologies such as text messaging for tracking purposes, cameras for data collection, and their ability to use cellular networks for Internet connection, enable mobile devices to act as an ideal platform for the delivery of health services [47]. Determining the exact location through employing positioning technology, is also helpful for emergency situations [78] and device comfort purposes [55].

Poket Doktor System(PDS) is one of the primary architectures in this area. This system includes an electronic patient device which contains electronic health care records, health care provider devices and communication links between them [83]. One of the major uses of mobile devices in health care is for monitoring purposes. Intelligent mobile health monitoring system (IMHMS) [75], introduces an architecture which is a combination of 3 main parts. Through a wearable body network, the system collects data and sends it to the patient's personal network. This network logically decides whether to send the information to an intelligent medical server or not. The intelligent medical server is monitored by the specialist. Due to the broadness of the field different monitoring systems have been introduced for specific purposes.

2.1.2 Privacy

Deploying information systems in the health care area has resulted in higher efficiency and quality of care [39]. At the same time, these systems have contributed to some challenges including privacy and access control. [48] determines five major factors

which impact on privacy.

- Establishment of policy and regulations and implementing them.
- Production of in need hardware and software.
- Distribution and management system.
- Public key infrastructures.

Some architectures have been introduced in order to improve privacy in health care area. [86] presents a security capsule with token management architecture in order to have secure transmission and data storage on device. Some models also worked on access control for health care systems based on the user's behaviours [91]. In [93] the authors recognize the increasing need for protection of resources in information systems in networked environments. They propose a framework to minimize the risk of unauthorized access whilst supporting selective information sharing in role-based systems. The framework utilizes delegations as a means to propagate access to protected resources by trusted users. However, this model considers only access issues to the information and it does not look at information flow.

2.2 Trust Models in Health care Information Systems

The use of Trust Models in electronic health care can be classified into two groups: sharing information and electronic health records and monitoring patients. [18] introduced Cassandra, a trust management system that is flexible in the level of ex-

pressiveness of the language by selecting an appropriate constraint domain. Also, they present the results of a case study, a security policy for a National Electronic Health Record system, demonstrating that Cassandra is expressive enough for large-scale real-world applications with highly complex policy requirements. They identify implementation steps including; building a prototype, testing the EHR policy in a more realistic setting, and producing web-based EHR user interfaces [18]. This model is also interested only in access control policies and cannot act as a decision support tool for the user.

Considering the importance of security in wireless data communication, [23] reviews the characteristics of a secure system and proposes a trust evaluation model for health care systems. Data confidentiality, authentication, access control and privacy are examples of mentioned security issues. In this system, nodes are representative of each component of the system. A trust relationship between nodes has been evaluated to determine the trustworthiness of each node. The main difference between this system and other related works is that the trust value of each node is computed based on an exponential function. This leads to an increase of past behaviour impact on trust [23]. This model only calculates trust based on its past behaviour and it does not consider the preferences of the user.

2.3 Trust Management

Advances in technology and communication systems have contributed to change in many areas including commerce, information sharing, storing and communication. Because of this, deciding to share information with other parties or buying and selling through online systems has become a controversial issue. Trust Management is an approach to deal with this problem.

Trust has roots in social sciences and can be defined as the degree of subjective belief about the behaviours of another party [20]. Trust management computerizes in some way the human notion of trust. Using formalized trust many models have been developed for different applications such as healthcare [21], telecommuting [37], mobile computing [88] and electronic commerce [45].

2.3.1 Definition of Trust

Trust plays an important role in people's daily lives. Without trust, efficiency and dynamism would decrease [36]. Moreover, society may become in danger of collapse [22]. However, there is no identical definition of trust for everyone [59]. Trust can be studied from different perspectives, depending on the person whom defines trust and the type of trust [56]. In addition, there is wide spectrum of literature for defining trust since trust has been studied in different fields such as evolutionary biology [17], sociology [51], social psychology [27], economics [38], history [32] and philosophy [49]. Looking at trust from the psychological point of view, Morton Deutch's definition of

trust is one of the most accepted. In [26], he states that, when an individual is in an ambiguous path, two conditions might happen. The first path might contribute to beneficial event (V+) while the other one might lead to a harmful one (V-). If occurrence of each event depends on the other party and the possibility of occurrence of the (V-) is greater than the possibility of occurrence of (V+), and the person still chooses the harmful path, he made a trust decision [26].

In sociology, Luhmann's definition of trust is widely accepted. He describes trust as a tool to reduce the complexity of life [50]. Likewise, Bernard Barber, has a sociological view of trust. Moreover, there is an element of future expectations in his definition of trust. According to Barber, "trust is expectation of the persistence and fulfillment of the natural and moral social order. He added two more expectations which are: 1. Expectations of technically competent role performance from those we interact with in social relationship and systems and 2. Expectations that a party would have from the other party in an interaction in order to do their obligations and responsibilities [16]. Gambetta is one of the scientists who holds a multidisciplinary view of trust. He defines trust as a particular level of subjective probability. For instance, in a scenario where an agent assesses another agent or group of agents, the agent will perform a particular action both in a situation before monitoring the action or in a context which he can monitor actions [32].

According to the literature, trust is conceptual and depending on the situation can have different meanings. This will contribute to different models of trust for different

uses and also different trust models for the same purpose [60].

2.3.2 Computing Trust

Trust has been studied in various fields and can be deployed based on context. However, society is common theme in all areas. Whether we are living in a society and playing our roles as actual human beings or we are in virtual world and interacting with other agents, we need trust to survive [22]. The need of trust in virtual society, leads to formalizing trust. The idea of formalizing a concept or behaviour is not new. Philosophers and artists such as Plato, Aristotle, and Michelangelo attempted to mathematically formalize different behaviours.

There are different ways for computing behaviour, specifically trust, and considerable research has done in the area.

Terminology

Some terms are needed in order to be used in formalizing trust:

Entities: Entities are subjects and objects of trust relationship. They can be elements of trust decision such as people or agents.

Trust Value: The trust value is a numeric value assigned to trust and it is used to measure the degree of trust [70].

The term Trust Management as introduced by Blaze is a unified approach to specifying and interpreting security policies, credentials relationships which allows direct authorization of security-critical actions [20].

Sources of Information

Trust models consider different sources of information to calculate trust value. Some of them only take into account “traditional” sources such as experiences and observations. These models take into account previous interactions with the other party. Also, it is possible for them to witness interactions of the party in question with other agents [71]. More complex models also consider sociological aspects of agent to calculate a trust value. As in the real world, in virtual societies each agent has roles. The trust relationship between the agents is based on their sociological relationship and the role that they are playing in the society at that time [71]. Capturing social relation data is possible by various methods such as social network analysis. However, this kind of analysis depends on the availability of relational data [74]. Using this data it possible to calculate trust value for social partners.

Trust and Reputation Models

The earliest model of computerized trust was the one proposed by Marsh [56]. He considered three types of trust in his model.

- **Basic trust** which is calculated based on all accumulated experiences of an agent.
- **General trust** which is an estimate of trust in an agent without considering a specific situation.
- **Situational trust** which is an estimate of trust in an agent considering a

specific situation.

Calculating trust value both based on the agents itself and also their situation is the basis of our trust model as well. The use of reputation models is common in online market places such as Amazon Auctions and eBay [62]. eBay, for example, uses a reputation mechanism in which users are able to give three values: positive, negative and neutral, to their transaction. eBay calculates the reputation value as the sum of the values over the previous six months [3]. Likewise, Amazon calculates the reputation value based on the average value of the reviews [1]. In this case their sources of information are only based on witness information (information from previous transactions).

Evolving these kind of reputation models, Sporas was introduced [92]. This model considers the rating of the most recent interaction of two parties. Moreover, users with very high reputation values experience fewer changes after each update in comparison to users with low reputation values. In comparison to other reputation models, this one is more robust to changes in the user's behavior [92]. Schillo et al [72], proposed a trust model in which the result of an interaction is good or bad and there is no level of satisfaction. This model is based on probability theory. Thus, the model calculates the amount of trust that agent A gives to agent Q as in the probability that agent Q will be honest. Esfandiari and Chandrasekharan proposed a model based on two one-on-one acquisition mechanisms [30]. In the first method they use Bayesian network to perform trust acquisition and in the second trust acquisition method is based on

interaction. Generally, there are two protocols of interactions. *Exploratory protocol* where the agents ask other agents about known things to evaluate their degree of trust, and *querycontrol* where agents may ask advice from trusted agents [30].

In [63], the authors developed a trust-based algorithm for a messaging system. In this algorithm, each node has been assigned a trust value based on its behaviour. At the same time, each message was divided into 4 parts and only nodes with the total trust value were able to read all parts of the messages. However, the nodes themselves, were not categorized based on their trust value.

Reviewing the state of art shows that although various models have been introduced, they scarcely address context. Moreover, the models are mostly deciding only based on the requestor not the preferences of the owner of the information. These issues, highlight the need for a comprehensive trust model.

2.3.3 Trust, Privacy and Security

Security mechanisms protect systems from non-authorized parties. There are some challenges that are not addressed by traditional methods. Traditional methods, usually limits the access for authorized users. However, detecting authorized requestors is a complex issue in information sharing. Moreover, information providers might also mislead users by providing false information. These types of problems can be addressed by trust models [42].

2.3.4 Comfort

Comfort, is defined as “A feeling of relief or encouragement, a satisfying or enjoyable experience” [85]. Device comfort is concept that uses a notion of trust to let a personal device better reason about an interaction and suggest decision. Context and behaviour of the users are some of the influential factors on comfort level [54]. As an information security methodology, device comfort can act as a perfect tool for protecting health care information. [55] introduced a three layer architecture which can reason about sharing of medical information for based on context.

Based on this feel of comfort, the device makes decisions. In this research, the comfort level is used by device in order to decide about a sharing situation. The device tries to know the user, their likes and dislikes and their behaviors in different situations. Using this data, the device can reason that in which scenarios, user would trust and vice versa.

2.4 Conclusions

Investigating healthcare information sharing models, showed that privacy models aim to address general concerns for information privacy [89]. However, privacy is also situation specific [73]. Then, it is significant to distinguish between general privacy and context based privacy. Furthermore, several pioneering studies examined general privacy risks and few frameworks specifically designed for mobile privacy issues [90].

Moreover, privacy and security models in health applications results in limitation

of performance [13]. This raises the need of privacy models with no significant effect on the performance of the application while it addresses the privacy concerns of the user.

Reviewing the state of the art, highlighted that there is a need for comprehensive trust model specifically in health. Considering current issues, a contextual trust model can perfectly act as a security tool in this area. In the next chapter, we review Apple Healthkit framework as an example of a platform which connects mobile health applications.

Chapter 3

Apple's HealthKit Framework

3.1 Overview

Mobile devices and applications have been reviewed from various aspects such as security [24], privacy [13], medical implications [65], user implications [87], software engineering [61]. In addition to mobile health applications itself, new platforms such as Apple HealthKit were introduced which enable the health apps to connect to each other [6]. However, mostly the focus of the research in this area is on the functionality of the application and information security is only scarcely addressed [25]. In this chapter, we review the process model of Health Kit design in addition to current privacy issues in this area.

3.2 HealthKit Design

The HealthKit framework, which was introduced by Apple in iOS 8, lets health and fitness applications as well as smart devices gather health information about a user in one location. The framework provides services in order to share data between health and fitness applications. Through the HealthKit framework different applications can get access to each other's data with the user's permission. Users also can view, add, delete and manage data in addition to edit sharing permission using this app [6]. The framework can automatically save data from compatible Bluetooth LE heart rate monitors and the M7 motion co-processor into the HealthKit store [5].

In order to provide applications with data, HealthKit contains some predefined lists which constrain the data type and units. Moreover, HealthKit produces hierarchical subclasses of data [5].

Each data item can be stored inside the HealthKit store is called a HealthKit object (HKObject). Each HKObject has the following properties:

- **UUID:** A unique identifier for the particular entry
- **Source:** The source of data
- **Metadata:** A dictionary which contains additional information about the entry.

HKObjects fall into two categories: characteristics and samples. Characteristics represent data which does not change over time, such as blood type and biological sex. Samples are data that change over time. A sample object describes data at specific

time and has properties including type, start date and end date.

3.2.1 HealthKit Store

All of the data that is managed by HealthKit is linked through the HealthKit store. Each application needs to use the HealthKit store in order to request and get permission for reading and sharing the health data [7]. There are different methods to access data in the HealthKit store:

- Direct Method Calls: Through this method direct access to characteristic data is possible. Direct Method Calls can be only used for this type of data.
- Sample Query: This general-purpose query can be used to access any type of sample data. They are specifically useful for sorting results or limiting the number of samples returned.
- Observer Query: This long running query can monitor the HealthKit store and inform the user if any changes occur in matching samples.
- Anchored Object Query: Used in order to find out the newest samples which have been added to the store. On the first run, it will bring all the matching samples and in the following it will only bring the newer data.
- Statistics Query: Used to perform statistical calculations over the samples.
- Statistics Collection Query: Through this query, multiple statistics queries can be performed over a period of fixed length time intervals.

- Correlation Query: Used to for complex searches of data.
- Source Query: Used to search for the similar applications and sources which use the same matching sample data [5].

All the health applications can store their collected data in HealthKit store. At the same time, if another application asks such information, it can have access to it. This model, does not consider the differences between the requestor applications and their purpose of use. Figure 3.1 shows an example interface of HealthKit.

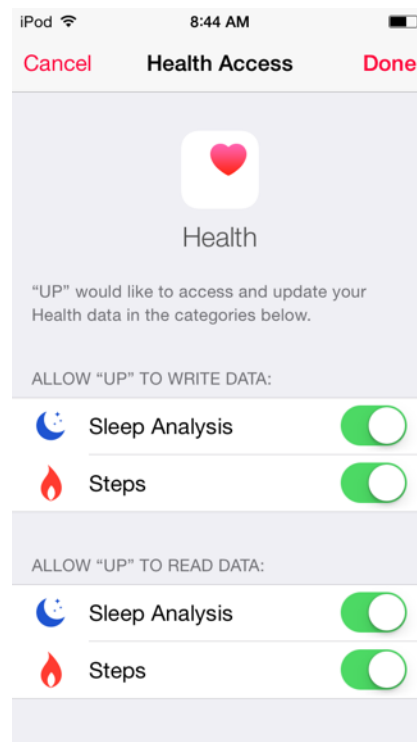


Figure 3.1: Example of Apple HealthKit interface

3.3 Privacy in HealthKit

Currently each application is individually responsible for obtaining the trust of the user in order to get access to their health information. Users can decide whether to share data with that specific app or not. Users can also share some part of data whilst not giving permission for sharing another part [5].

In order to maintain the privacy of a user's data any application in the HealthKit must have a privacy policy. Personal health records model and HIPAA guidelines can be used in order to create these policies [5]. However, there is no control over data when it is stored in the store.

3.4 Privacy in mHealth

mHealth systems are aimed to improve the quality of care and quality of life, however, they generate privacy and security issues [12]. Privacy is important in any healthcare information system, however, some factors differentiate mHealth. mHealth, allows for more data collection. For example, by mobile applications ECG of a patient can be recorded continuously for two weeks rather than a one minute recording every two weeks. Moreover, mHealth can collect broader data about the patient. Applications collect information about patient's lifestyle and activities, locations and food. Also, mHealth, provide the ability of information sharing with a wide spectrum of people, including the healthcare system, insurance companies and other application [13]. In this setting privacy is complex. The patient needs control over collection, recording

and access to their health data [13].

Concern's about one's privacy varies among the human population [13]. These concerns impede a user's willing to share their information [19]. Furthermore, breach of security and privacy of health information not only result into manipulation and leakage of sensitive data, but also it might bring serious consequences like worsen morbidity or death [13]. Considering current privacy issues in the area of health care, in addition to definitions of privacy in this sector, raises the need of a tool which can act as a decision support system for the user.

3.5 Conclusion

Privacy in this context is critically important as there is a large volume of personal information on the network. New frameworks such as Apple HealthKit provide the opportunity of sharing health information between various applications. However, when information becomes available in the store, it can be stored and shared with any requester despite the reputation level of the requester. Moreover, Apple's model of privacy does not categorize the information for specific purposes. It also, does not consider the reliability of the requestor applications. These facts highlight the need of a model for health information sharing, which can address the privacy issues.

In the next chapter, we introduce the B-trust model which can act as a decision support tool in mHealth area.

Chapter 4

The B-Trust Model

In this chapter, we introduce B-Trust, a trust model that considers both personal and contextual aspects the user of the application. This model is intended to be used by the owner of the information to make decisions about sharing their health (or indeed, any) information, or part of it, with a specific application. The model acts as a decision support tool for sharing information by category, purpose and context, taking into account differences in the behaviour of users, various third parties who are seeking for the information, and environmental conditions. After describing the working process of the model, each component of the model is presented. Figure 4.1 shows a conceptual overview of the model's working process. For example, Tracy as a user, has a specific comfort level for sharing her fitness information for research purposes. She is willing to share her information after a week passed of data collection. Based on this information ($C_{fitness}$, $P_{research}$, T_{week}), the model would calculate a trust level (T),for the collected information.

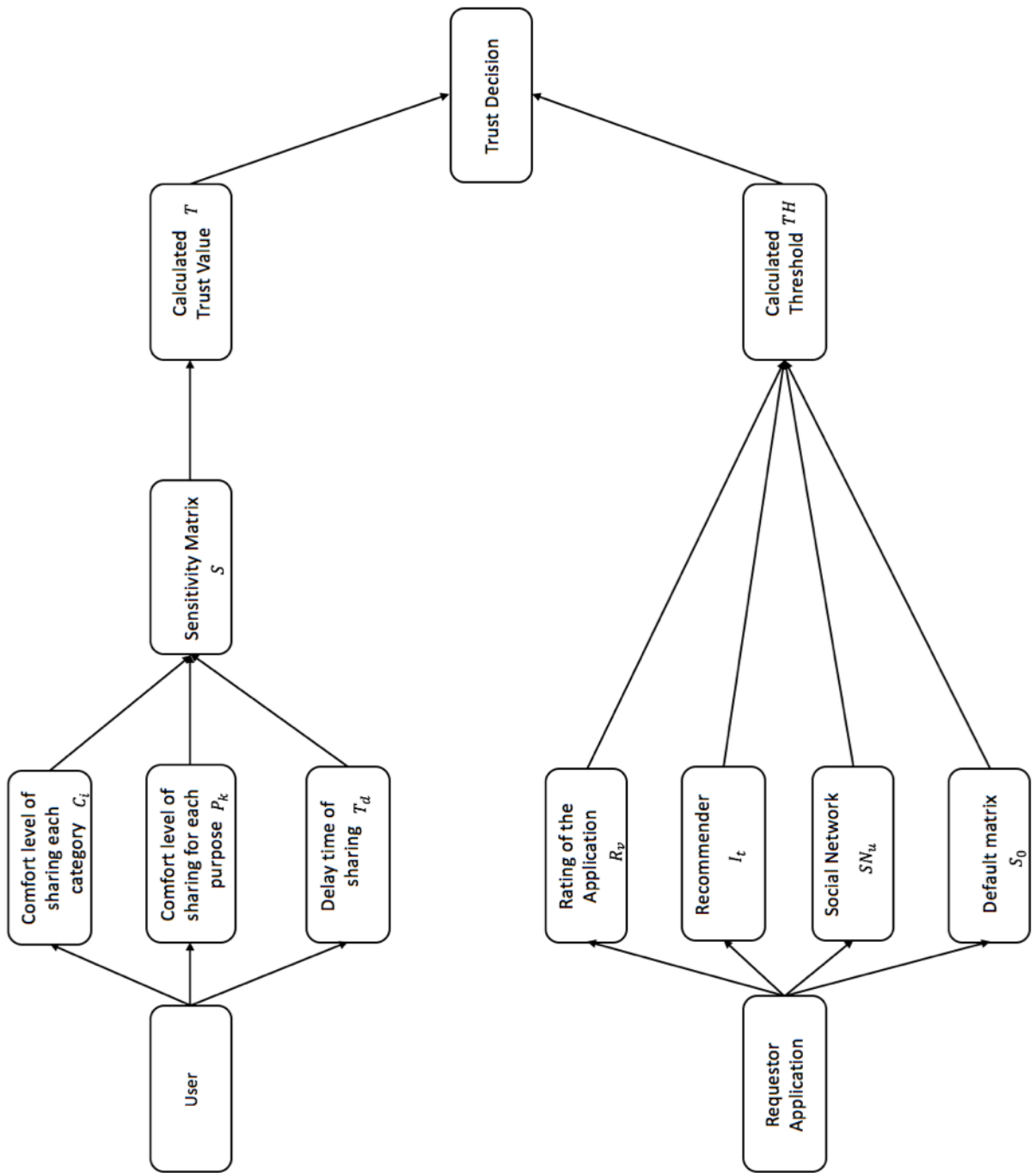


Figure 4.1: Architecture of B-trust model

On the other hand, a requestor application of such information ($C_{fitness}, P_{research}$), would be evaluated based on factors such as its rating, R_v , recommender (I_t). Moreover, the number of trusted users of the application (who have installed it) is influential on this evaluation. For instance, two of Tracy's friends on social network are using the same application. In the end, the threshold for this application (TH), would be calculated. If this threshold can reach user's trust level (T), the information would be shared. Otherwise, the requestor application cannot get access to this information.

4.1 Calculation of the Trust Value for Specific Types of Information

Personal dispositions and experiences such as current health status and risk beliefs have an impact on the individual decision making process [15]. To address and calculate the trust value for each purpose of information, there are two components which must be calculated. The first component of the model calculates the amount of trust that each person needs for sharing a specific part of the information. In previous example, Tracy's trust level addresses this value. The amount of trust that already exists between a device and the application which is asking for the information is calculated through the second component of the model. Again, in the provided example the calculated threshold addresses this value. In the end, by comparing the two values, advice on sharing the information is given. We consider a scenario in

which information has been categorized based on its type in the health care sector.

At the time of calculation of the trust value by the first layer of the model, we assume that there is no user knowledge of the application which is seeking the information.

Table 4.1 summarizes the notations used in this chapter.

Table 4.1: Explanation of Notations

Symbols	Explanation
S	Sensitivity of information
C	Category of information agent
j	The index of information categories
n_c	Number of information categories
A	Application agent
i	The index of applications
P	Purpose of use of information
k	The index of user purposes
m_p	Number of usage purposes
S_{i_0, j_0}	Basic threshold
T_d	Recency of information
C_0	Default Trust value for all of the categories
P_0	Default Trust value for all of the purposes
R	Rating of application agent
v	Representative of application rating
SN	Social network agent
u	Representative of number of mutual friends
I	Installer of the application agent
t	Representative of the installer of the application
TH	Threshold for information sharing
T	Trust value

4.2 The Personal Perspective

People's behaviour about information sharing varies [41]. Stone and Stone [82] explored the links between the personality of individuals and information privacy issues. Gefen et al. [34] determined that personality has an impact on trust in virtual environments. Moreover, past experiences of the user can have a crucial impact on their trust level [58]. The personal perspective layer of the model will calculate the amount of trust that the user requires in the application in order to share the information or a specific part of it. This layer is based on the preferences of the owners of the information. To formalize the proposed system, this research considers a scenario in which a specific part of health information of a user has been requested by a specific application. In order to determine the privacy preferences of each user, various factors should be considered and specific trust values need to be assigned. In the following sections, these factors and the methodology of assigning the trust values are presented.

4.2.1 Sensitivity of Information

Information sensitivity might differ for individuals [64, 67, 68]. For example, some people share their information more than others. Formation of beliefs and behaviours has roots in personality [11]. Research also suggests a relation between personality traits and sensitivity of health information for individuals [28]. To facilitate the subjectivity of the sensitivity of each piece of health information for users, we give

the user the chance for decision making for each piece of information. The most significant factors which have an impact on the calculation of the trust value are explored in the following section.

Category of Information

The type of information requested is influential on an individual’s privacy concerns and their willingness to share [84]. According to Gates and Whalen [33], people deliberately treat certain classes of information in a similar way. Accordingly, classifying related information in the same cluster, enables the user to behave similarly towards them. Consequently, in this research, health information is classified based on both type and transformability (See table 4.3).

Some health information can alter over its lifetime. In our model, we used the Apple HealthKit categories which fall into two main groups. The first group, “characteristic data” refers to data which does not change over time such as gender, blood type and date of birth. The second group of data is the that which has been collected through the device and might change over time [5,6].

Table 4.3: Information Categories

Characteristic Data	Sample Data
Biological sex	Vital signs
Blood type	Sleep analysis
Date of birth	Body measurements
Fitzpatrick skin type	Fitness
	Nutrition

In our model, C_j represents different categories of information. For each category of information, users would assign a “comfort” value for sharing each category of information. This value would be between $(-1,+1)$. The average value of the provided number could be calculated through the following formula:

$$Mean_{c_j} = \frac{1}{n_c} \sum_{i=1}^{n_c} C_j \quad (4.1)$$

For example, when Tracy assigns different comfort values for each type of her information such as $(C_{fitness}, C_{vitalsign})$, $Mean_{c_j}$ would calculate the average comfort level. This value is useful in section 4.3.

Purpose of use of information:

Recent studies in the Knowledge Management area highlight the need for the user to have control over their information [69]. Put simply, the owners of the information should have the answer to the question: “Who knows what” [69]. As well, the scope of health care applications is as extensive as medicine itself [81]. Since personal information sharing norms vary within different networked groups [29], in this research, applications which are seeking information are categorized based on the purpose for using that information. For instance, as current health status of individuals have a personal impact on the sensitivity of information [15], users might be unwilling to share their information for any purpose but personal health monitoring.

Considering existing applications in health care, the aim of the use of information

can be categorized into at least one of several groups. The following groups are some of the examples of these purposes.

- Personal Monitoring: A great portion of mHealth applications are designed to monitor health status of the users [57].
- Public health Monitoring: Health applications can use people's information for the sake of improvement of the health status of another user.
- Research: Many mHealth applications are designed for medical research purposes [57].
- Commercial Usage: The Health Insurance Portability and Accountability Act (HIPAA) allows many businesses to have access to individual's health information [10]. It is obvious that there is a need to have access to an individual's health information for some businesses, such as insurance companies, however, information should not be shared without consent, even for improving health care delivery or ease of care.
- Governmental Usage: Ministry of health and long-term care may collect and use personal health information [9].

In our model we use A_i to represent these categories, thus, for each application depending on its purpose, A_i , would be an element of at least one of the following sets:

$$A_i \in P_k \tag{4.2}$$

in which:

$$k = \left\{ \begin{array}{l} \textit{Research} \\ \textit{Personal Monitoring} \\ \textit{Public Health Monitoring} \\ \textit{Commercial Usage} \\ \textit{Governmental Usage} \end{array} \right.$$

Depending on the personality and priorities of the users, they might be more or less interested in sharing information for each purpose. For each purpose again, users would assign a “comfort” value for sharing the information.

The average value of the provided number could be calculated through the following formula:

$$Mean_{P_k} = \frac{1}{m_p} \sum_{k=1}^{m_p} P_k \tag{4.3}$$

For example, when Tracy assigns different comfort values for each different purpose of uses such as $(P_{\textit{Research}}, P_{\textit{Personalmonitoring}})$, $Mean_{P_k}$ would calculate the average comfort level. This value is useful in section 4.3.

This kind of classification not only helps the user to have control over their information, but also encourages them to allow the use of their information or part of

it for a specific reason which they might disapprove of if they would need to make a general consent.

Sensitivity Matrix

We use a matrix in order to represent and determine the relationships between various categories of information and purposes of use. In this $m_p \times n_c$ matrix, columns represent categories and rows represent purposes. Each element of the matrix is the minimum number of the assigned (by the user, but with some defaults) comfort value for a specific purpose and category.

$$S_{j,k} = \min(C_j, P_k)$$

$$S_{c_j, p_k} = \begin{bmatrix} s_{1,1} & s_{1,2} & \cdots & s_{1,n_c} \\ s_{2,1} & s_{2,2} & \cdots & s_{2,n_c} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m_p,1} & s_{m_p,2} & \cdots & s_{m_p,n_c} \end{bmatrix} \quad (4.4)$$

Through this matrix, the system is able to choose a specific part of information for a specific purpose, instead of omitting a whole category of information. For example, consider Tracy as a user. She is not willing to share her vital sign information with an application which has commercial purposes. So, she gives a lower comfort rate to

this purpose, therefore, her information won't be shared with commercial application.

At the same time, she can share her information for research purposes.

If the purpose of the application which is asking for the information is unclear, average of assigned values for all purposes could be used as a trust value.

$$Mean_{P_k} = \frac{1}{m_p} \sum_{k=1}^{m_p} P_k \quad (4.5)$$

4.2.2 T_d : Delay Time

Time plays a dominant role in the level of sensitivity of information [35]. Accordingly, it is possible to say that level of sensitivity of the information decreases for the owner as the interval of capturing information and sharing it increases. Consequently, this factor is added in order to address the privacy of the user. Users can decide on sharing part(s) of their information after a specific delay. This may result in a decrease in sensitivity of information for the user. Users have 3 options for sharing, representing different time periods before information is released. Depending on the user's preference, T_d would be equal to:

$$T_d = \begin{cases} 1.5, & \text{if Share immediately} \\ 1, & \text{if Share after one week} \\ 0.5, & \text{if Share after one month} \end{cases} \quad (4.6)$$

Then:

$$S = f(C, P, T_d) = T_d \cdot \begin{bmatrix} s_{1,1} & s_{1,2} & \cdots & s_{1,n} \\ s_{2,1} & s_{2,2} & \cdots & s_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m,1} & s_{m,2} & \cdots & s_{m,n} \end{bmatrix} \quad (4.7)$$

For example, if Tracy decides to share her information after a month, her trust level increases.

4.3 Context Perspective

The second component of the model examines the context of a user at the time of giving permission for sharing the information with regard to the requestor application. In other word, this component of the model, calculates a trust rate for the requestor application of information which is the amount of trust that already exists. The criteria for this calculation are:

- Default Trust to the applications in question
- The application's reputation based on its current rating
- Common friends in social networks using the application
- The person who suggested installation of the application, for example health care provider versus an old friend

In the model, a higher amount of existing trust results in a lower sharing threshold.

4.3.1 Default trust to each category and purpose

Since at the beginning there is no information on specific applications, the mean trust value which was assigned by the user would be used as the sensitivity matrix. By using this matrix, a basic trust threshold can be defined for each user. The mean is chosen as a measure for central tendendancy, as it considers all comfort values in the calculation in comparing to the mode and median.

C_0 = Default Trust value for all of the categories

P_0 = Default Trust value for all of the purposes

In order to optimize the trust value, the minimum value of C_0 and P_0 would be selected as each element of the S_0 matrix. By considering the minimum value, the model would suggest more realistic decisions as it considers the lowest acceptable comfort level of the user.

$$S_{j_0, k_0} = \min\left(\frac{1}{n_c} \sum_{i=1}^{n_c} C_j, \frac{1}{m_p} \sum_{i=1}^{m_p} P_k\right) \quad (4.8)$$

then:

$$S_0 = \begin{bmatrix} \min(C_0, P_0) & \min(C_0, P_0) & \cdots & \min(C_0, P_0) \\ \min(C_0, P_0) & \min(C_0, P_0) & \cdots & \min(C_0, P_0) \\ \vdots & \vdots & \ddots & \vdots \\ \min(C_0, P_0) & \min(C_0, P_0) & \cdots & \min(C_0, P_0) \end{bmatrix} \quad (4.9)$$

Each element of this matrix is the minimum amount of C_0 and P_0 . Minimum is chosen to optimize the comfort levels in order to reflect the trust value.

4.3.2 Application Rating (public social)

Application distribution platforms let individuals buy and sell mobile applications. Moreover, these platforms provide them an opportunity to share their experiences through rating scores. User-driven quality assessment is possible using these feedbacks. Higher application ratings have positive effects on download numbers and vice versa [66]. This factor is considered in our model. R_v represents the rating score of the application in our model, for a specific online rating of v . Considering who is seeking for the application, R_v would have one of the following values:

$$R_v = \begin{cases} 0.5, & \text{if } v > \text{average} \\ 1, & \text{if } v < \text{average} \\ 2, & \text{if } v < 0 \end{cases} \quad (4.10)$$

4.3.3 Social network friends

Friends and family have a potentially strong influence on people's decision making processes [79]. Likewise, when it comes to decision making in virtual communities such as e-commerce, research suggests that individuals trust their family and friends more than strangers [79]. As well, [46] recognizes that there is an increase in volume

of traffic to retail websites through social networks such as MySpace and Facebook. Accordingly, the factor of social networks added is considered in the formula. The higher the number of friends who are using the same application is, the higher the amount of trust in the application would be.

SN_u represents the number of friends who are using the same application. Considering the number of friends in common SN_u would value one of the followings:

$$SN_u = \begin{cases} 0.5, & \text{if } u > 5 \text{ mutual friends} \\ 0.75, & \text{if } 0 < u < 5 \text{ mutual friends} \\ 1, & \text{if } u = 0 \text{ mutual friend} \end{cases} \quad (4.11)$$

4.3.4 Installer of the Application:

In healthcare information systems, the relationship of the person who is asking for the information to the owner of information can have a critical impact on the existing level of trust between them [13]. For example, if a person involved in the patient care suggests an application, the application in question is seen as potentially more reliable. In our model, 3 scenarios are considered for installing an application. I_t represents the source suggesting the application. Considering who is seeking for the

application I_t would value one of the following:

$$I_t = \begin{cases} 0.5, & \text{if Healthcare provider suggests} \\ 0.75, & \text{if Applications compatible with wearable technology} \\ 1, & \text{if Randomly downloaded application} \end{cases} \quad (4.12)$$

4.3.5 Estimation of the Threshold

Considering all the factors discussed in section 4.3, calculated threshold would be:

$$TR = S_0 \cdot R_v \cdot SN_u \cdot I_t \quad (4.13)$$

If the calculated trust value of the user is higher than the calculated threshold value, then information would be shared for this category in this context.

$$TR < T \quad (4.14)$$

4.4 Conclusion

In this chapter, the B-Trust model was introduced. This model contains two main components. The model categorizes the information and its purpose of use of them. Then, the first component of the model calculates the trust level of the user for each category of information as well as for each purpose. By creating a relation between

information categories and purposes, the model calculates trust value of the first component.

The second component of the model, calculates the trust threshold of each requester application. Application rating, recommender of application and mutual social network users are influential in the calculation

At last, each category of information would have a trust value for each purpose. At the same time, each application requestor has a trust threshold for each category of information and its purpose of use of them. Trust decision is made by comparing these two values. If trust value is higher than the threshold, the information would be shared. Otherwise, the requestor application cannot have access to the information.

In the next chapter, different examples (consideration of different personalities and context) are provided to clarify the working process of the model.

Chapter 5

Theoretical Examples

Generally, the output of the model described in chapter 4 depends on 3 variables: the user, the user's context and the application which is requesting the information. In this chapter, in order to enhance understandability, we present various examples of personalities, situations and applications with reference to the model. We continue by providing 4 example scenarios. Lastly, we examine the proposed trust model in these scenarios.

5.1 Various Agents

Personality and characteristics of people have a crucial impact on their decision making. In order to make allowances for this, in this experiment we divide the user agents to three main categories: optimistic, pessimistic and realistic. In the following sections each category is described:

Optimist

An optimist believes in the best outcome in all the situations and expects the best results in everything [56]. In our examples, an optimist always selects the maximum trust value.

Pessimist

The pessimist expects the worst outcome in any situation. Therefore, the pessimistic agent selects the minimum trust value in all situations [56].

Realist

In reality, most people are some place between the two extremes. This situation can be also applied to agents. For the sake of simplicity in this paper, we randomly choose from intervals within the 4 quartiles in the spectrum from optimist to the pessimist.

5.2 Pool of Applications

In healthcare environments, various applications with different characteristics exist.

This section looks at applications with these different characteristics:

Application α

Application α has the following characteristics:

- It needs to have access to nutrition information, fitness information and vital signs.
- It uses information for commercial purposes, research purposes and also personal health monitoring.
- It has been rated less than average of rating of the similar applications by the mobile users.

Application β

Application β has the following characteristics:

- This application needs access to sleep analysis information and nutrition information.
- It uses information for research purposes, personal health monitoring and public health.
- It has been rated higher than average of rating of the similar applications by the mobile users.

Application γ

Application γ has the following characteristics:

- This application needs access to sleep analysis information and vital signs.
- It uses information for research purposes and personal health monitoring

- The rating of the application is not specified. (Consequently, it is considered that the application does not have any rating.)

Application δ

Application δ has the following characteristics:

- This application needs access to all of health types of health information
- It uses information for research purpose, commercial uses and personal health monitoring
- This application has been rated negatively.

5.3 Various Situations

Although personality plays a significant role in decision making other factors, including the experiences of the user or their state of mind can affect judgment. To clarify, if the model works as expected in various situations, we test the model in 4 different scenarios. In this part, we examine our model using different scenarios as use case examples. Furthermore, different user personalities and various applications have been considered.

Examining model in various situations and considering different users with different personalities, demonstrates the usability of the model in different scenarios.

5.3.1 Scenario 1– Installing Random Applications

Tracy was browsing health care applications on the app store. One of the diet applications interested her and she installed it on her device. She did not have any past information about this application, no one has suggested it and none of her friends are using this application. This application needs to have access to her fitness and nutrition information.

5.3.2 Scenario 2 – Various Rated Applications

Steve is a tech savvy person. He reads reviews of applications and downloads many health apps onto his device. Rating of the applications is the most effective reason for him to decide to download the application or not. Furthermore, he is willing to share his information for research purposes or for monitoring his own health. However, Steve is not interested in sharing for commercial uses. Recently, he has sleeping problems. He is looking for a sleep analysis application to install.

5.3.3 Scenario 3– Installing Applications Suggested by Trusted Persons

Bob goes to a walk in clinic to consult his doctor because of his sleeping problem. After discussing the issue and symptoms of Bob, the doctor recommends that he starts using a new wearable device in order to analyse his sleep information. This smart device allows Bob's doctor real time access to information and sleep tracking.

Bob needs to install the compatible application with this device on his phone in order to be able to send the information in addition to wearing the device every night when he sleeps. This application allows researchers to access to the information with a built in delay, in addition to Bob's doctor.

5.3.4 Scenario 4- Share Everything

During the past few months Julia had different cardinal symptoms. Her doctor asked her to use a wearable device, in order to monitor her and diagnose her disease. As a result, she is very nervous about her condition, she downloads many applications randomly to share her information with. She did not pay attention to the purpose of which application asks for her information. She expects that all of her information will be shared in order to get faster results.

5.4 Mathematical Analysis

In order to illustrate how the model works, in this section we briefly analysis the model for the scenarios outlined above.

Scenario 1.

In the first scenario, we consider Tracy to be an optimist. Therefore, she assigns a higher trust value for sharing information. Table 5.1 represents the trust values she assigned for each purpose and category.

Table 5.1: Trust Values Assigned by Tracy

Information Category	Trust value	Purpose	Trust value
Vital signs	0.81	Research	0.22
Sleep analysis	0.32	Personal monitoring	0.31
Body measurements	0.46	Public health	0.46
Fitness	0.22	Commercial Usage	0.51
Nutrition	0.33	Governmental usage	0.73

In the sensitivity matrix we have the minimum amount between each category and purpose, therefore:

$$S = f(C, P) = \begin{bmatrix} 0.22 & 0.22 & 0.22 & 0.22 & 0.22 \\ 0.31 & 0.31 & 0.31 & 0.22 & 0.31 \\ 0.46 & 0.32 & 0.46 & 0.22 & 0.33 \\ 0.51 & 0.32 & 0.46 & 0.22 & 0.33 \\ 0.73 & 0.32 & 0.46 & 0.22 & 0.33 \end{bmatrix} \quad (5.1)$$

$$t_d = 1.5 \quad (5.2)$$

Based on equation 5.1 and equation 5.2, the trust matrix would be:

$$S_{m,n} = \begin{matrix} & \begin{matrix} VitalSigns & SleepAnalysis & Bodymeasurements & Fitness & Nutrition \end{matrix} \\ \begin{matrix} Research \\ PersonalMonitoring \\ PublicHealth \\ CommercialUsage \\ GovernmentalUsage \end{matrix} & \left[\begin{array}{ccccc} 0.33 & 0.33 & 0.33 & 0.33 & 0.33 \\ 0.46 & 0.46 & 0.46 & 0.33 & 0.46 \\ 0.69 & 0.48 & 0.69 & 0.33 & 0.49 \\ 0.76 & 0.48 & 0.69 & 0.33 & 0.49 \\ 1.09 & 0.48 & 0.69 & 0.33 & 0.49 \end{array} \right] \end{matrix} \quad (5.3)$$

We consider that that application α is the application which Tracy has downloaded. Therefore, for equation 4.9 we have:

$$S_{i_0,j_0} = \min\left(\frac{1}{5} \sum_{i=1}^5 C_j, \frac{1}{5} \sum_{i=1}^5 P_k\right) = \min(0.428, 0.444) = 0.428 \quad (5.4)$$

$$S = f(C, P) = \begin{bmatrix} 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \\ 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \\ 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \\ 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \\ 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \end{bmatrix} \quad (5.5)$$

And:

$$R_v = 1 \quad (5.6)$$

$$SN_u = 1 \quad (5.7)$$

$$I_t = 1 \tag{5.8}$$

Then, the threshold matrix would be:

$$TR = \begin{bmatrix} 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \\ 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \\ 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \\ 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \\ 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \end{bmatrix} \tag{5.9}$$

Specific parts of information for specific purposes are expected to be shared if the value of corresponding member of sensitivity matrix is higher than the value of corresponding member in the threshold matrix. Therefore, fitness information won't be shared since the trust value is less than the threshold. However, nutrition information and vital signs information will be shared since for the purpose in which application α using this information, trust value is higher than the threshold.

$$0.33 < 0.428 \rightarrow \textit{Do not share} \tag{5.10}$$

$$0.46 > 0.428 \rightarrow \textit{Share vital signs information for personal monitoring} \tag{5.11}$$

Table 5.2: Trust Values Assigned by Steve

Information Category	Trust value	Purpose	Trust value
Vital signs	-0.31	Research	-0.22
Sleep analysis	-0.68	Personal monitoring	0.11
Body measurements	0.23	Public health	-0.47
Fitness	-0.46	Commercial Usage	-0.86
Nutrition	-0.33	Governmental usage	-0.59

Scenario 2

In the second scenario, we consider Steve to be a pessimist. He does not give high trust values to the application. Therefore, he assigns the following trust values as noted in table 5.2.

In the sensitivity matrix we have the minimum amount between each category and purpose, therefore:

$$S = f(C, P) = \begin{bmatrix} -0.31 & -0.68 & -0.22 & -0.46 & -0.33 \\ -0.31 & -0.68 & 0.11 & -0.46 & -0.33 \\ -0.47 & -0.68 & -0.47 & -0.47 & -0.47 \\ -0.86 & -0.86 & -0.86 & -0.86 & -0.86 \\ -0.59 & -0.68 & -0.59 & -0.59 & -0.59 \end{bmatrix} \quad (5.12)$$

Steve decides to share his information after one week.

$$t_d = 1 \quad (5.13)$$

Then the trust matrix would be:

$$S_{m,n} = \begin{matrix} & & \textit{VitalSigns} & \textit{SleepAnalysis} & \textit{Bodymeasurements} & \textit{Fitness} & \textit{Nutrition} \\ \textit{Research} & \left[\begin{array}{ccccc} -0.31 & -0.68 & -0.22 & -0.46 & -0.33 \\ -0.31 & -0.68 & 0.11 & -0.46 & -0.33 \\ -0.47 & -0.68 & -0.47 & -0.47 & -0.47 \\ -0.86 & -0.86 & -0.86 & -0.86 & -0.86 \\ -0.59 & -0.68 & -0.59 & -0.59 & -0.59 \end{array} \right. \\ \textit{PersonalMonitoring} & & & & & & \\ \textit{PublicHealth} & & & & & & \\ \textit{CommercialUsage} & & & & & & \\ \textit{GovernmentalUsage} & & & & & & \end{matrix} \quad (5.14)$$

We consider that that application β is the application which Steve has installed.

Therefore, we have: (From equation 4.9)

$$S_{i_0, j_0} = \min\left(\frac{1}{5} \sum_{i=1}^5 C_j, \frac{1}{5} \sum_{i=1}^5 P_k\right) = \min(-0.31, -0.406) = -0.406 \quad (5.15)$$

$$S = f(C, P) = \begin{bmatrix} -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \\ -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \\ -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \\ -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \\ -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \end{bmatrix} \quad (5.16)$$

And:

$$R_v = 1 \quad (5.17)$$

$$SN_u = 1 \quad (5.18)$$

$$I_t = 1 \tag{5.19}$$

The the threshold matrix would be:

$$TR = \begin{bmatrix} -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \\ -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \\ -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \\ -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \\ -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \end{bmatrix} \tag{5.20}$$

Again, by comparing matrix elements, a recommended decision for information sharing can be made.

$$-0.68 < -0.406 \rightarrow \textit{Do not share} \tag{5.21}$$

$$-0.33 > -0.406 \rightarrow \textit{Share nutrition information for research} \tag{5.22}$$

$$\textit{laberlnut2} - 0.33 > -0.406 \rightarrow \textit{Share nutrition information for personal monitoring} \tag{5.23}$$

$$-0.47 < -0.406 \rightarrow \textit{Do not share nutrition information} \tag{5.24}$$

The calculated trust value is less than threshold for nutrition information (equation 5.22), these information for research purposes and personal monitoring. However, these information won't be shared as application β uses them for public health pur-

Table 5.3: Trust Values Assigned by Bob

Information Category	Trust value	Purpose	Trust value
Vital signs	0.16	Research	0.26
Sleep analysis	0.18	Personal monitoring	0.21
Body measurements	0.28	Public health	-0.39
Fitness	0.02	Commercial Usage	0.32
Nutrition	- 0.11	Governmental usage	-0.16

poses. Trust value of nutrition information for this value is less than calculated threshold. For the same reason, sleep analysis information won't be shared with the application β .

Scenario3.

In the third scenario, we consider Bob considered to be a realistic. Consequently, he assigns moderate trust values for sharing his information. Moreover, as he realizes the importance of time of sharing with his doctor he agrees to immediate share of his information. Table 5.3 represents the trust values she assigned for each purpose and category.

In the sensitivity matrix we have the minimum amount between each category and

purpose, therefore:

$$S = f(C, P) = \begin{bmatrix} 0.16 & 0.18 & 0.26 & 0.02 & -0.11 \\ 0.16 & 0.18 & 0.21 & 0.02 & -0.11 \\ -0.39 & -0.39 & -0.39 & -0.39 & -0.39 \\ 0.16 & 0.18 & 0.28 & 0.02 & -0.11 \\ -0.16 & -0.16 & -0.16 & -0.16 & -0.16 \end{bmatrix} \quad (5.25)$$

$$t_d = 1.5 \quad (5.26)$$

Then the trust matrix from equation 4.9 would be:

$$S_{m,n} = \begin{matrix} & & \textit{VitalSigns} & \textit{SleepAnalysis} & \textit{Bodymeasurements} & \textit{Fitness} & \textit{Nutrition} \\ \textit{Research} & \left[\begin{matrix} 0.24 & 0.27 & 0.39 & 0.03 & -0.16 \\ 0.24 & 0.27 & 0.31 & 0.03 & -0.16 \\ -0.58 & -0.58 & -0.58 & -0.58 & -0.58 \\ 0.24 & 0.27 & 0.42 & 0.03 & -0.16 \\ -0.24 & -0.24 & -0.24 & -0.24 & -0.24 \end{matrix} \right. \\ \textit{PersonalMonitoring} & \\ \textit{PublicHealth} & \\ \textit{CommercialUsage} & \\ \textit{GovernmentalUsage} & \end{matrix} \quad (5.27)$$

We consider that application γ is the application which Bob's doctor has suggested and he downloaded, therefore we have:

$$S_{i_0, j_0} = \min\left(\frac{1}{5} \sum_{i=1}^5 C_j, \frac{1}{5} \sum_{i=1}^5 P_k\right) = \min(0.106, 0.048) = 0.106 \quad (5.28)$$

$$S = f(C, P) = \begin{bmatrix} 0.106 & 0.106 & 0.106 & 0.106 & 0.106 \\ 0.106 & 0.106 & 0.106 & 0.106 & 0.106 \\ 0.106 & 0.106 & 0.106 & 0.106 & 0.106 \\ 0.106 & 0.106 & 0.106 & 0.106 & 0.106 \\ 0.106 & 0.106 & 0.106 & 0.106 & 0.106 \end{bmatrix} \quad (5.29)$$

And:

Rating of the application considered less than average.

$$R_v = 1 \quad (5.30)$$

Also, none of Bob's friends are using this application.

$$SN_u = 1 \quad (5.31)$$

Finally, as the application has been suggested by the health care provider we have:

$$I_t = 0.5 \quad (5.32)$$

Then the threshold matrix from equation 4.13 would be:

$$TR = \begin{bmatrix} 0.053 & 0.053 & 0.053 & 0.053 & 0.053 \\ 0.053 & 0.053 & 0.053 & 0.053 & 0.053 \\ 0.053 & 0.053 & 0.053 & 0.053 & 0.053 \\ 0.053 & 0.053 & 0.053 & 0.053 & 0.053 \\ 0.053 & 0.053 & 0.053 & 0.053 & 0.053 \end{bmatrix} \quad (5.33)$$

Specific parts of information for specific purposes are expected to be shared if the value of corresponding member of sensitivity matrix is higher than the value of corresponding member in the threshold matrix. In this scenario, as the requester of the information is the health care provider, it is expected that sleep analysis information be shared. As we know application γ is asking for sleep analysis information in addition to vital sign information.

$$0.27 > 0.053 \rightarrow \textit{Share sleep analysis information for personal monitoring} \quad (5.34)$$

$$0.27 > 0.053 \rightarrow \textit{Share sleep analysis information for research} \quad (5.35)$$

Scenario 4.

In the fourth scenario Julia is devastated and she downloaded many different applications. In this case it is expected by Julia that her information be shared with her

Table 5.4: Trust Values Assigned by Julia

Information Category	Trust value	Purpose	Trust value
Vital signs	0.98	Research	0.8
Sleep analysis	0.93	Personal monitoring	0.94
Body measurements	0.84	Public health	0.93
Fitness	0.30	Commercial Usage	0.7
Nutrition	0.21	Governmental usage	0.52

doctor immediately. On the other hand, as Julia has downloaded random applications, it is expected that the model only shares information with those applications which are asking for monitoring purposes. Julia has cardinal symptoms, consequently she only needs to share her vital sign information with the other applications. In this scenario, as Julia shares everything, she is considered to be optimist person for the purpose of this example. Therefore, she relatively assigns a higher trust value for sharing information. Table 5.4 represents the trust values she assigned for each purpose and category.

In the sensitivity matrix we have the minimum amount between each category and purpose, therefore:

$$S = f(C, P) = \begin{bmatrix} 0.8 & 0.8 & 0.8 & 0.3 & 0.21 \\ 0.94 & 0.93 & 0.84 & 0.30 & 0.21 \\ 0.93 & 0.93 & 0.84 & 0.30 & 0.21 \\ 0.70 & 0.70 & 0.70 & 0.30 & 0.21 \\ 0.52 & 0.52 & 0.52 & 0.30 & 0.21 \end{bmatrix} \quad (5.36)$$

$$t_d = 1.5 \tag{5.37}$$

Then the trust matrix based on equation 4.7 would be:

$$S_{m,n} = \begin{matrix} & \begin{matrix} VitalSigns & SleepAnalysis & Bodymeasurements & Fitness & Nutrition \end{matrix} \\ \begin{matrix} Research \\ PersonalMonitoring \\ PublicHealth \\ CommercialUsage \\ GovernmentalUsage \end{matrix} & \begin{bmatrix} 1.2 & 1.2 & 1.2 & 0.45 & 0.31 \\ 1.41 & 1.39 & 1.26 & 0.45 & 0.31 \\ 1.39 & 1.39 & 1.26 & 0.45 & 0.31 \\ 1.05 & 1.05 & 1.05 & 0.45 & 0.31 \\ 0.78 & 0.78 & 0.78 & 0.45 & 0.31 \end{bmatrix} \end{matrix} \tag{5.38}$$

We consider that that application γ is the application which Julia's doctor recommended her to download. Therefore:

$$S_{i_0,j_0} = \min\left(\frac{1}{5} \sum_{i=1}^5 C_j, \frac{1}{5} \sum_{i=1}^5 P_k\right) = \min(0.652, 0.778) = 0.652 \tag{5.39}$$

$$S = f(C, P) = \begin{bmatrix} 0.652 & 0.652 & 0.652 & 0.652 & 0.652 \\ 0.652 & 0.652 & 0.652 & 0.652 & 0.652 \\ 0.652 & 0.652 & 0.652 & 0.652 & 0.652 \\ 0.652 & 0.652 & 0.652 & 0.652 & 0.652 \\ 0.652 & 0.652 & 0.652 & 0.652 & 0.652 \end{bmatrix} \tag{5.40}$$

And:

$$R_v = 1 \tag{5.41}$$

$$SN_u = 1 \tag{5.42}$$

Since Julia’s doctor suggested this application, then:

$$I_t = 0.5 \tag{5.43}$$

Then the threshold matrix based on equation 4.13 would be:

$$TR = \begin{bmatrix} 0.326 & 0.326 & 0.326 & 0.326 & 0.326 \\ 0.326 & 0.326 & 0.326 & 0.326 & 0.326 \\ 0.326 & 0.326 & 0.326 & 0.326 & 0.326 \\ 0.326 & 0.326 & 0.326 & 0.326 & 0.326 \\ 0.326 & 0.326 & 0.326 & 0.326 & 0.326 \end{bmatrix} \tag{5.44}$$

In this scenario since the downloaded application has been recommended by Julia’s doctor, the threshold is low in spite of the fact that the application’s rating is not specified. As:

$$1.41 > 0.326 \rightarrow \textit{Share sleep analysis information for research} \tag{5.45}$$

$$1.2 > 0.326 \rightarrow \textit{Share vital signs information for personal monitoring} \tag{5.46}$$

As we expected, the requested information would be shared with this application.

Scenario 5.

In the fourth scenario, in addition to the application γ , which was recommended by Julia's doctor, she downloaded several applications randomly. As was mentioned before, because of Julia's anxiety she did not put any effort into finding "good" applications. Here, we consider that she downloaded application δ . It is expected that the trust model should be able to recognize that this application does not need to have access to all Julia's information. Also, it would not be surprising if the model does not let Julia share her information. Julia's trust value for information sharing are mentioned in Table 5.4. Therefore, her sensitivity matrix based on equation 4.7 would be:

$$S = f(C, P) = \begin{bmatrix} 0.8 & 0.8 & 0.8 & 0.3 & 0.21 \\ 0.94 & 0.93 & 0.84 & 0.30 & 0.21 \\ 0.93 & 0.93 & 0.84 & 0.30 & 0.21 \\ 0.70 & 0.70 & 0.70 & 0.30 & 0.21 \\ 0.52 & 0.52 & 0.52 & 0.30 & 0.21 \end{bmatrix} \quad (5.47)$$

$$t_d = 1.5 \quad (5.48)$$

Then the trust matrix based on equation 4.9 would be:

$$S_{m,n} = \begin{matrix} & \begin{matrix} VitalSigns & SleepAnalysis & Bodymeasurements & Fitness & Nutrition \end{matrix} \\ \begin{matrix} Research \\ PersonalMonitoring \\ PublicHealth \\ CommercialUsage \\ GovernmentalUsage \end{matrix} & \left[\begin{array}{ccccc} 1.2 & 1.2 & 1.2 & 0.45 & 0.31 \\ 1.41 & 1.39 & 1.26 & 0.45 & 0.31 \\ 1.39 & 1.39 & 1.26 & 0.45 & 0.31 \\ 1.05 & 1.05 & 1.05 & 0.45 & 0.31 \\ 0.78 & 0.78 & 0.78 & 0.45 & 0.31 \end{array} \right] \end{matrix} \quad (5.49)$$

Application δ is asking for Julia's information:

$$S_{i_0,j_0} = \min\left(\frac{1}{5} \sum_{i=1}^5 C_j, \frac{1}{5} \sum_{i=1}^5 P_k\right) = \min(0.652, 0.778) = 0.652 \quad (5.50)$$

$$S = f(C, P) = \begin{bmatrix} 0.652 & 0.652 & 0.652 & 0.652 & 0.652 \\ 0.652 & 0.652 & 0.652 & 0.652 & 0.652 \\ 0.652 & 0.652 & 0.652 & 0.652 & 0.652 \\ 0.652 & 0.652 & 0.652 & 0.652 & 0.652 \\ 0.652 & 0.652 & 0.652 & 0.652 & 0.652 \end{bmatrix} \quad (5.51)$$

And:

$$R_v = 2 \quad (5.52)$$

$$SN_u = 1 \quad (5.53)$$

$$I_t = 1 \tag{5.54}$$

Then the threshold matrix based on the equation 4.13 would be:

$$TR = \begin{bmatrix} 1.3 & 1.3 & 1.3 & 1.3 & 1.3 \\ 1.3 & 1.3 & 1.3 & 1.3 & 1.3 \\ 1.3 & 1.3 & 1.3 & 1.3 & 1.3 \\ 1.3 & 1.3 & 1.3 & 1.3 & 1.3 \\ 1.3 & 1.3 & 1.3 & 1.3 & 1.3 \end{bmatrix} \tag{5.55}$$

As we can, the application does not let Julia to share her information for most of the purposes. However, her sleep analysis information would be shared with the application. The reason is that, she assigned higher trust values for her sleep analysis information.

$$1.39 > 1.3 \rightarrow \textit{Share sleep analysis information for research} \tag{5.56}$$

5.5 Conclusion

In this chapter, we provided 5 example scenarios to illustrate how the B-Trust model, proposed in chapter 4, works. In these examples, users have different personalities. Also, the requester applications are various.

The results of each example explain the working process of the model with regard

to the requester application and user.

In the next chapter, we introduce the “trust reasoning” application which is built based on the model introduced in chapter 4. Following by evaluation of the model through a study.

Chapter 6

Experiment: Investigating the Impact of the Trust-reasoning Interface on Users

This chapter discusses the evaluation phase of the proposed model in order to verify its usability and understandability. For this aim, we designed an interface, which reflects various aspects of the model. The model was examined through the “trust-reasoning” interface in an experiment. The study aimed to illustrate the understandability of the model, the level of the satisfaction of the user as well as the clarity of its difference in comparison to current frameworks.

The experiment was submitted and approved by the Research Ethics Board at UOIT on May 1st 2016 under REB 15-106.

6.1 Use of User Study as an Evaluation Method

A large body of work on use of trust models for different contexts has been previously done. To the best of our knowledge, evaluation methods for most of these models were limited to simulation studies. The simulation process is effective, whilst the goal of the study is capturing differences of specific performances of an element between two or more models. However, these methods of evaluation do not include the opinion of the user about the trust models or their understandability. Looking at the issue from a privacy perspective, the user's opinion on the ability of the machine to represent their preferences has great importance, and cannot be examined through simulation. To this end, we designed a user study through which the opinion of users regarding the trust model can be captured.

6.2 Evaluation Goals

The intention of carrying out the initial experiment was to investigate the performance of the model from the user's perspective. More specifically, the study was designed to explore the impact of the use of the trust-reasoning interface on the user and determine whether the differences between this interface and other interfaces is recognizable by the user or not. Moreover, the study examines the impact of the application on the user's awareness of privacy.

6.3 Application Design and Development

Aiming to illustrate the working process of the model, an application example has been developed based on the proposed trust model. This application is developed on iOS 10.11.15 with the Swift programming language, for iPhones. Through the first three screens, the application collects some information in order to be able to calculate the trust level of the user for sharing health information. On the last screen, users are shown their trust level. It is also possible for them to edit their information at this stage. The following section explains input and output of each screen.

6.3.1 User Interface











The user interface was designed to gather basic information from users regarding their priorities for information sharing, to allow our model calculate their level of trust in other circumstances. It also illustrates to the users their level of trust. [80]'s guideline suggests the following five main principles for displaying the data.

- Consistency in data display,
- Efficient information assimilation by the user,
- Minimal memory load on the user,
- Compatibility of data display with data,
- Flexibility for user control of data display,

6.3.2 User Interface Design Criteria

Visualization has great impact on improving simplicity [77]. To meet the principles of [80] as well as boosting clarity and simplicity, categories of information and the purposes of information use are represented by symbolic icons. Table 6.1 shows the icons which were used in the interface.

Table 6.1: Explanation of icons were used in the interface

Icons	Explanations	Icons	Explanations
	Vital signs Information		Monitoring Personal health
	Fitness Information		Monitoring Public health
	Sleep Information		Research
	Body measurement information		Commercial
	Nutrition Information		Governmental

Use of sliders for capturing data results in ease of use in addition to clarity of representation of the estimated value by user [31]. The following criteria are what we aim for:

- Simplicity
- Generality
- Comprehensibility

From the main interaction styles, direct manipulation was chosen. The direct manipulation interaction style is easier to learn and reduces errors in comparison to the



Figure 6.1: A screen shot of vital signs information slider

other methods [77]. Symbolic icons are placed on the slider to point the level of trust for each piece of information. Different levels of trust are shown by various colors on the slider. Color selection aims to resemble the risk of sharing. Using symbolic icons on a colorized slider, results in faster and easier interaction. An example of such a slider, that is designed for the trust reasoning application, is shown in figure 6.1. The slider has the ability of capturing various values on a spectrum.

Screen 1- Figure 6.2

The first screen of the application is designed to capture user's comfort level for sharing their health information. Through sliders, users are able to input their comfort level. The higher the comfort level, the higher probability of sharing might be. The application notifies the user of higher risks by changing the color of the slider (figure 6.2).

Screen 2- Figure 6.2

In the second screen of the application users are asked to show their comfort level for sharing their health information for different purposes. Users can choose their level of comfort through sliders. Similar to information sliders, purpose sliders are able to notify user the risk of sharing by changing their color. (Figure 6.2)



Figure 6.2: The “category of information” input screen

Screen 3- Figure 6.4

This is the last screen in which users are asked to input values. At this screen time delays for sharing the application with the third party are asked from the user. Users have the option to share their information between immediately and, up to one month after the time that information was collected.

Screen 4- Figure 6.5

Based on the captured information through the last three screens, the application calculates the trust level of the users for sharing their information. The fourth screen, represents the results. If the user presses any of information buttons, the trust level

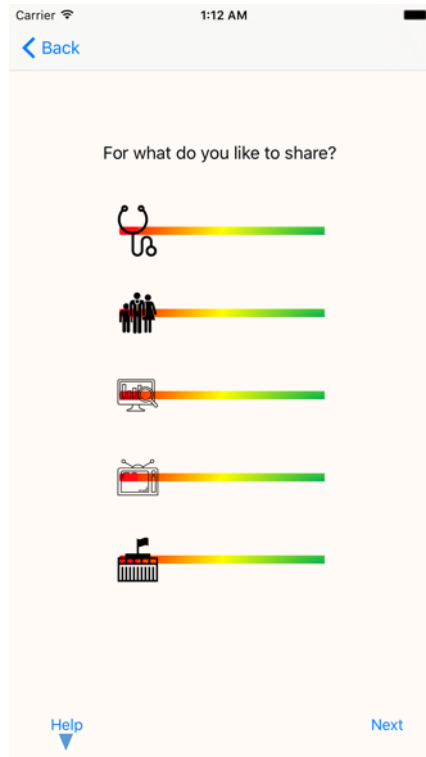


Figure 6.3: The “purpose of information” input screen

of each purpose appears on the sliders. It is possible for users to edit their threshold at this stage by using sliders.

The input of the users to the first three pages of the application is their comfort level for sharing. The application calculates a trust level for each purpose category based on these comfort levels. Using comfort levels, the device can better reason about a situation and suggest a decision. More specifically, the trust-reasoning application uses these comfort level to suggest trust value for the first component of the application.

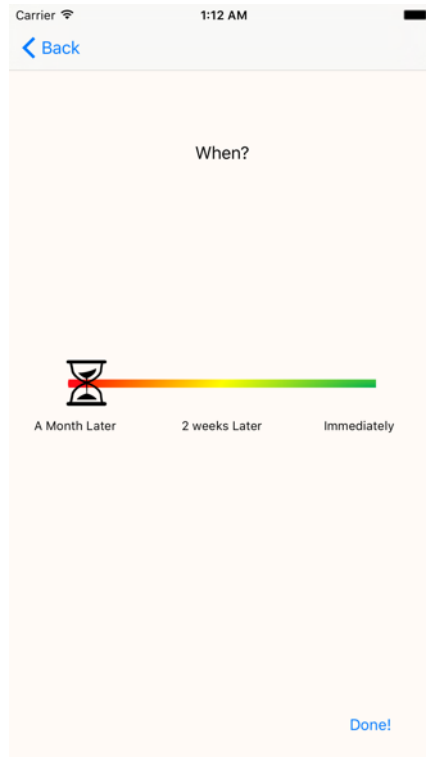


Figure 6.4: The delay time input screen

6.4 Methodology

6.4.1 Experimental Environment

The study was conducted in person at UOIT. The experiment was designed as a single session study and participants were not required to perform any task outside of the session. Also, there was no special requirement from the participants. An experimenter was in the room at all time.

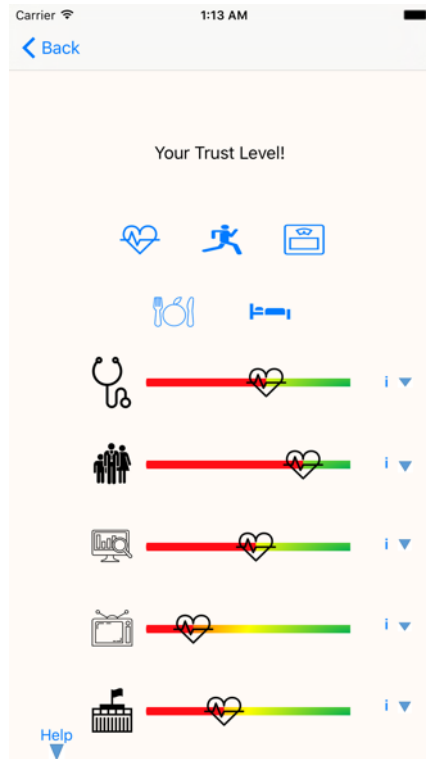


Figure 6.5: Fourth screen- Results

6.4.2 Participants

Data was collected from a total of 44 participants. The age of the sample population ranged from 18 to 34. Participants were enrolled voluntarily and did not receive any compensation. Invitation letters were distributed on campus to invite students to participate in the study. Participating students were recruited from various majors and levels of study.

6.4.3 Procedure

A within-participant study was adopted and each participant interacted with trust reasoning application and Apple Health interface. The order participants were in-

teracting with applications was counterbalanced to account for any possible learning effect that may occur. In total, data was collected from 44 participants.

The letter of invitation, shown in Appendix 7.1, was distributed in the university in order to attract students to participate in the study. Participants were welcomed to the laboratory and a summary of the procedure were explained to them. After the explanation of the tasks, consent was obtained. Once they had no further questions, participants were shown the interface followed by a questionnaire. In the second part they were shown the trust-reasoning application which is based on the proposed model and at the first screen they were asked to illustrate their level of comfort for sharing each category of information through the slider. The help button was designed in order to clarify the meaning of the icons for the users. Through the second screen, users were asked how comfortable they were for sharing their information for each purpose, followed by the third screen in which participants were able to illustrate their preferred time of sharing. The last screen illustrates, based on their input, what is their trust level for each category and purpose. Following this, participants were asked to fill out the last questionnaire.

Apple Health Questionnaire

In order to collect data regarding the experience of the user with the healthcare applications, a questionnaire was used. The questionnaire was designed to provide context on participants experience to better interpret the findings of the experiment, and involved 9 questions. The first two questions addressed the age and gender. The

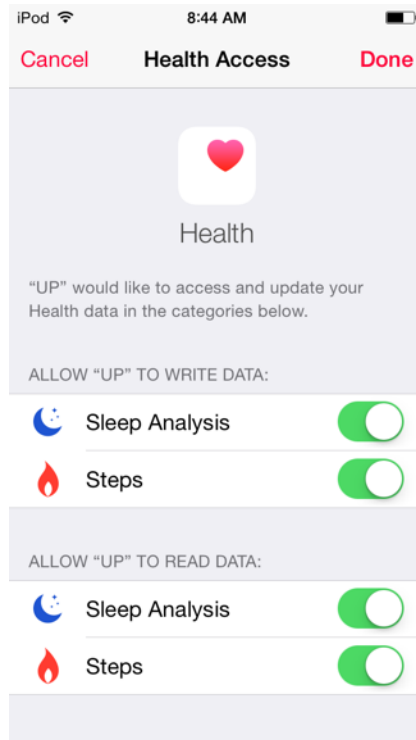


Figure 6.6: Example of Apple HealthKit interface

following seven questions referred to the participant's opinion on privacy of health information and their experience with apple health interface. Appendix 7.2 shows the questionnaire.

Trust reasoning App Questionnaire

In order to determine the satisfaction of the user with the experiment the second questionnaire shown in Appendix 7.3 was designed. This questionnaire aims to quantify the level of user satisfaction with trust-reasoning application. Moreover, the questionnaire highlights the clarity of differences of the proposed interface to the current one. This questionnaire involved 11 questions, the first two questions addressed the age and gender and the following seven questions are similar to the Apple Health

questionnaire referring to the participant's experience with the trust-reasoning interface. This questionnaire, has also two additional questions regarding the performance of the application. These questions focus on clarity of the application performance based on the model.

6.4.4 Questionnaire Design

In (Q1) participants were asked about their perception of privacy in regard to their health information. The purpose of this question was to examine the relationship between the framework that participants use and their perception about privacy. (Q2), (Q3) and (Q5) investigate the relationship between the application that users are using and their comfort level for collection and sharing of their information. (Q4) and (Q9) are interested in user's opinion about the application that they are using. This is important for estimation of user satisfaction. Through (Q6) and (Q7), it is possible to find out the user's satisfaction regarding the beneficiary of the application. Lastly (Q8) asks about the clarity of the application performance for users.

6.4.5 Results

For both applications, 44 users answered questions based on a 5-point Likert scale based on level of agreement for each question. Survey results for the first question showed that participant's perception of privacy is significantly higher in using the first trust reasoning application than the old interface. This is shown in the following

Table 6.2: Likert scale answers

Q1	Privacy of my information is very important for me.
5	Strongly Agree
4	Agree
3	Neither agree nor disagree
2	disagree
1	Strongly disagree

ANOVA analysis in which the parametric assumptions were satisfied.

A two condition analysis of variance (ANOVA) with 2, (Trust reasoning App vs Apple App) x 7 (question types) repeated measures conducted on the user's preference was performed (Figure 6.7). There was a significant main effect of application ($F(1,43)=29.84, p < 0.001$) such that the trust reasoning application had a higher satisfaction than the Apple application. There was also a significant main effect of question type ($F(6,43)=35.11, p < 0.001$). However, the results show that there is no significant interaction between applications and questions ($F(6,43)=0.434, p < 0.001$). Following the significant main effects of the questions factors, we conducted a post hoc pairwise t-tests using the false discovery rate (FDR) correction for multiple comparison. There was no significant difference in the post-hoc t-test between the mean response level of the following questions: 1 vs 7, 4 vs 6, 2 vs 5, 5 vs 5, 5 vs 6, 6 vs 7, 4 vs 5 and 2 vs 4. Between all other questions there was a significant difference in response, which is shown in Table 6.4.

An important difference was captured between question 1 (mean response = 4.23) and 6 (mean response= 3.61) for which there was a significant difference ($p < 0.05$)

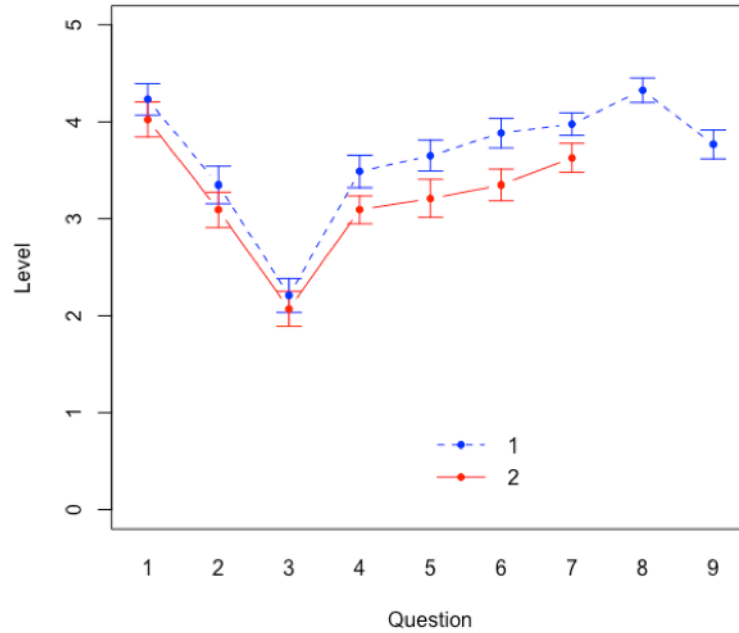


Figure 6.7: Description of ANOVA- App 1: Trust-reasoning, App 2: Apple Health-Figure illustrates that the score mean of all answers for Trust reasoning application is higher than Apple application. Score of answers to question 3 has the lowest mean.

due to the fact this question showed important qualitative difference in the apps.

Figure 6.8 represents the interaction between the application used by a user (x-axis) and the average in the reported answers for each application. It is clear from figure 6.8 that there is a decrease in the response level, i.e, users had a higher degree of satisfaction with the trust reasoning application.

6.5 Discussion

The goal of this study was to investigate the user’s opinion on the privacy of collection and sharing of their health information. We compared the Apple-like interface for

Table 6.4: Correlation (Pearson’s R) of Questions

	1	2	3	4	5	6	7	8
2	$2.2e - 07$	–	–	–	–	–	–	–
3	$< 2e - 16$	$5.0e - 10$	–	–	–	–	–	–
4	$1.5e - 06$	0.6917	$3.7e - 11$	–	–	–	–	–
5	$6.9e - 05$	0.2545	$1.2e - 13$	0.4341	–	–	–	–
6	0.0040	0.0278	$< 2e - 16$	0.0676	0.3017	–	–	–
7	0.0676	0.0011	$< 2e - 16$	0.0040	0.0366	0.3017	–	–
8	0.3693	$2.3e - 07$	$< 2e - 16$	$1.3e - 06$	$3.0e - 05$	0.0011	0.0177	–
9	0.0998	0.0133	$2.5e - 14$	0.0291	0.1229	0.4814	0.8630	0.0278

health application to the trust-reasoning app which represents the B-trust model introduced in chapter 4 through a user study. The study aimed to answer the following questions:

- **RQ1:** Privacy of my information is very important for me.

H0 The *Apple Health* does have a positive impact on user’s comprehensiveness about privacy.

H1 The *Trust reasoning Application* has a positive impact on user’s comprehensiveness about privacy.

- **RQ2** I feel safe when my phone collects my information.

H0 The *Apple Health* does have a positive impact on the user’s comfort level for collection of their health data by their smart phone.

H1 The *Trust reasoning Application* does have a positive impact on the user’s comfort level for collection of their health data by their smart phone.

- **RQ3** I feel comfortable while I am sharing my information with the applications that I have no knowledge of them.

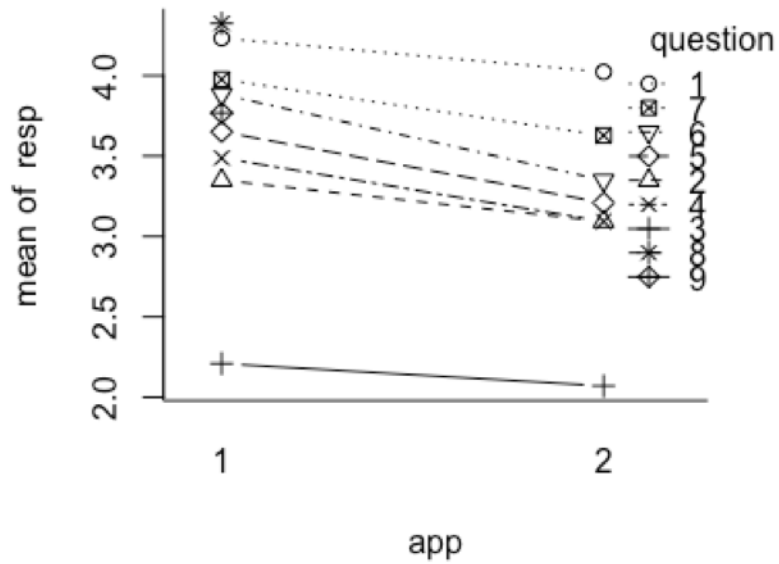


Figure 6.8: Description of MEAN Analysis - App 1: Trust-reasoning, App 2: Apple Health

H0 The *Apple Health* does have a positive impact on the user's comfort level for sharing their health data with the third party applications.

H1 The *Trust reasoning application* does have a positive impact on the user's comfort level for sharing their health data with the third party applications.

- **RQ4** I am satisfied with the current method of sharing of my information.

H0 The *Apple Health* does have a positive impact on the user's comfort level for sharing their health information.

H1 The *Trust reasoning Application* does have a positive impact on the user's comfort level for sharing their health information.

- **RQ5** I feel that I have control over sharing my information.

H0 The *Apple Health* does have a positive impact on the user's knowledge about their information behaviors towards health applications.

H1 The *trust reasoning application* does have a positive impact on the user's knowledge about their information behaviors towards health applications.

- **RQ6** I feel sharing my information is beneficial for my own health.

H0 The *Apple Health* does have a positive impact on the user's perception about the benefit of smartphones for their own health.

H1 The *Trust reasoning application* does have a positive impact on the user's perception about the benefit of smartphones for their own health.

- **RQ7** I feel sharing my information is beneficial for improvements in public health.

H0 The *Apple Health* does have a positive impact on the user's perception about the benefit of smartphones for improvements in public health.

H1 The *Trust reasoning application* does have a positive impact on the user's perception about the benefit of smartphones for improvements in public health.

- **RQ8** I understand how these interfaces work.

H0 Performance of the *trust-reasoning application* and how it addresses privacy is not clear for the user.

H1 Performance of the *trust-reasoning application* and how it addresses privacy is clear for the user.

- **RQ9** I am going to use these interfaces.

H0 User has low preferences in using *trust-reasoning application*.

H1 User has high preferences in using *trust-reasoning application*.

Each participant interacted with two applications and answered the same 7 questions for each study. Participants answered two additional questions about the trust-reasoning application. We found that participants had a higher level of satisfaction when they are using trust-reasoning application.

Analysis of the mean of the user's answers, illustrates that user's comprehensiveness of privacy of health information is high using both applications. The study showed that after using the trust-reasoning application they have a higher perception of privacy. The study showed that there is no interaction between the questions and applications. This points out that result of the study was dependent only on the change of application type (independent variable). Participants' mean of answer for the third question was the lowest, which shows that the user's willingness for sharing with an unknown third party application is low. However, users have a higher willingness for sharing with the application. Question 8 illustrates that the performance of the model was clear for the participants, also in comparison to other questions, participants reported a higher degree of agreement for this question. (Figure 6.9).

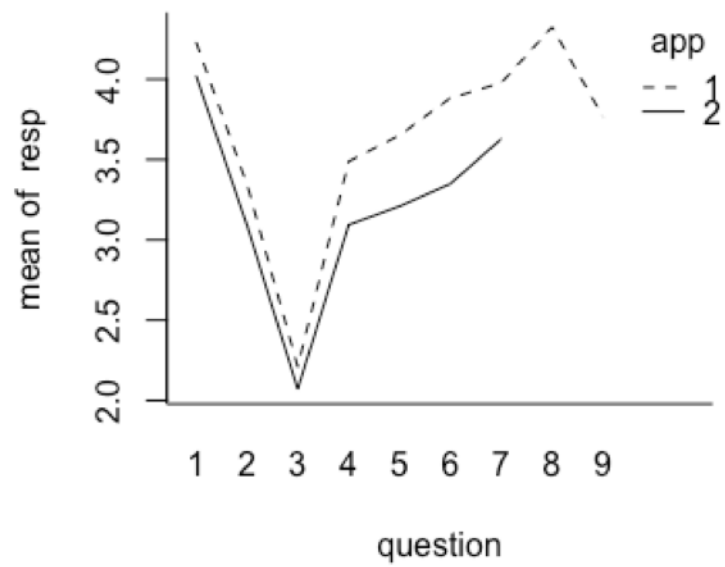


Figure 6.9: Description MEAN Analysis - App 1 = Trust reasoning, App 2= Apple Health

6.6 Limitations

The validity of this study is limited by participant selection. As the study was conducted on campus, participants age were between 18 to 44 years old. However, many users of mHealth are older adults. Also culture and education of the participants might have been effective in the study. In the future, these types of experiments should be conducted with recruiting participants from various cultures.

Furthermore, it is also possible that past experiences of the participants with Apple Health application has effect on the study. Moreover, user's medical history as well as user's immediate family member's medical history can have impact on decision making process of the user. Design and use of a similar interface to the Apple application instead of using the Apple application itself can reduce this confounding effect of the study.

6.7 Conclusion

In this chapter, an iOS application which is designed based on the B-Trust model is introduced. The application has four screens, of which the first three collects information regarding the sharing preferences of each category of information, different purpose of the collected information, and time delays. The last screen, presents the calculated trust level derived from the user.

To evaluate the model presented in chapter 4, a repeated measures study was designed based on the user's preferences.

A two-way condition (Trust reasoning App) and (Apple App) for the seven same questions repeated measures ANOVA was conducted on the user's preference. Results showed that users have higher mean level of satisfaction with the trust-reasoning application (mean response level = 3.54) vs the Apple app (mean response level = 3.2) across all the questions, which indicates that users are able to understand the performance of the trust model based on the application.

In the next chapter, we summarize the contributions of this research in addition to future work.

Chapter 7

Conclusions

We have shown that the B-Trust Model for designing the trust reasoning application was more successful in eliciting a higher level trust in comparison to the Apple app and it was more trustworthy from the user's perspective. For future work we aim to use a more advanced trust model.

7.1 Research Contributions

In this thesis, we discussed the current information systems in mHealth from privacy aspect. After highlighting the gaps in research in this area, weaknesses and strengths of the current systems were mentioned.

To address these issues, we introduced the B-trust model in chapter 4. The model is consist of two main components. The first component calculates the trust value for different categories of information for each user. Purpose of use of information

and time of sharing of the information is also considered in this calculation. The second component of the model, calculates the trust value of the requestor application. Rating of the application and its recommender are some of the factors which are influential in this valuation.

In chapter 5, to enhance understandability of the working process of the model, different scenarios were provided. These scenarios examine model in different contexts. Also it considers the variety of personalities of the users. The examination demonstrates the model's usability in different situation for various people.

In chapter 6, the trust reasoning application is introduced. This application is developed based on the B- trust model. The application has four screens. The first three screens are used to collect information from the user. The last screen represents the results. The application is examined in an experiment. The experiment was conducted at UOIT and 44 were participated. Results showed that users have higher satisfaction from privacy aspect using trust reasoning application. Results also illustrated that use of trust reasoning application contributes to higher awareness of privacy in compare to the Apple Health interface.

7.2 Future Work

There are a number of future research directions related to this topic:

- The proposed trust model for mHealth can be generalized for use in any information sharing scenario not specifically for healthcare.

- Also, a compatible extension of the application with smart watches can be built.
- Currently, in the B-trust model time factor represents the delay time between data collection and sharing. It is also important that consider the time of the availability of the information to the requestor. For example, the model gives access to the information to the requestor application for a week.
- Using machine learning techniques, the user's device can learn the comfort level of the users based on their behaviour and suggest sharing decisions based on that.

7.3 Conclusion

In this thesis, we investigated potential privacy issues in mobile healthcare area, and proposed a trust model which calculates the required trust value of information sharing between health care mobile applications, in relation to the existing amount of trust. By employing a trust model, we believe we can be proactive and prevent sharing parts of the information which put the privacy of the user in danger, whilst also giving ultimate control to the user. Moreover, by categorizing the information and purpose of use, we aim to provide an opportunity for sharing for different purposes. The model was evaluated theoretically through examination in several scenarios. Based on the model, an iOS application is designed and implemented which expresses the features of the B-trust model. We carried out a study to examine the model using

the application. Results showed that users have higher satisfaction using the trust reasoning application. Moreover, results illustrated that B-Trust model addresses privacy issues.

Appendix

Figure 7.1: Appendix 1- Invitation Letter



FACULTY OF BUSINESS AND
INFORMATION TECHNOLOGY

Research Participations Needed!

We are seeking individuals to participate in a research study in which I am comparing different decision making frameworks for information sharing between healthcare applications!

The experiment takes less than 30 minutes!



Who Can Participate?

Any University Student!

Contact Information:

If you are interested in participation in this research please contact:

Saghar Behrooz, MSc. in Computer Science Candidate

Principal investigator

Saghar.Behrooz@uoit.ca

This study is being conducted by Saghar Behrooz (principal investigator) and Dr. Stephen Marsh (Research Supervisor) at University of Ontario Institute of Technology and it has been approved by UOIT Research Ethics Board. (Reb #15-106)

Saghar.Behrooz@Uoit.ca
Saghar.Behrooz@Uoit.ca
Saghar.Behrooz@Uoit.ca
Saghar.Behrooz@Uoit.ca
Saghar.Behrooz@Uoit.ca
Saghar.Behrooz@Uoit.ca
Saghar.Behrooz@Uoit.ca
Saghar.Behrooz@Uoit.ca
Saghar.Behrooz@Uoit.ca
Saghar.Behrooz@Uoit.ca
Saghar.Behrooz@Uoit.ca
Saghar.Behrooz@Uoit.ca

Figure 7.2: Appendix 2- Apple Questionnaire

1. Please select your gender:

Female Male

2. Please select your age group:

15-19 20-24 25-29 30-34 35-40 41-45 46+ Other

Please indicate whether you agree or disagree with the statements provided.

(1= strongly disagree, 3=neither agree nor disagree, 5= strongly agree)

1- Privacy of my information is very important for me.

1 2 3 4 5

2- I feel safe when my phone collects my health care information.

1 2 3 4 5

3- I feel comfortable while I am sharing my information with the applications that I have no knowledge of them.

1 2 3 4 5

4- I am satisfied with the current method of sharing my information.

1 2 3 4 5

5- I feel that I have control over sharing my information.

1 2 3 4 5

6- I feel sharing my health information is beneficial for my own health.

1 2 3 4 5

7- I feel sharing my health information is beneficial for improvements in public health.

1 2 3 4 5

Figure 7.3: Appendix 3- BTHHealth Application Questionnaire



FACULTY OF BUSINESS AND
INFORMATION TECHNOLOGY

1. Please select your gender:

Female Male

2. Please select your age group:

15-19 20-24 25-29 30-34 35-40 41-45 46+ Other

Please indicate whether you agree or disagree with the statements provided.

(1= strongly disagree, 3=neither agree nor disagree, 5= strongly agree)

1- Privacy of my information is very important for me.

1 2 3 4 5

2- I feel safe when my phone collects my health care information.

1 2 3 4 5

3- I feel comfortable while I am sharing my information with the applications that I have no knowledge of them.

1 2 3 4 5

4- I am satisfied with the current method of sharing my information.

1 2 3 4 5

5- I feel that I have control over sharing my information.

1 2 3 4 5

6- I feel sharing my health information is beneficial for my own health.

1 2 3 4 5

7- I feel sharing my health information is beneficial for improvements in public health.

1 2 3 4 5

8- I understand how these interfaces work.

1 2 3 4 5

Figure 7.4: Appendix 3- BTHealth Application Questionnaire- Page 2

9- I am going to use this interface.

1 2 3 4 5

Bibliography

- [1] amazon. <http://www.Amazon.com>. Accessed: 2016-08-30.

- [2] Apple inc. healthkit. <https://developer.apple.com/healthkit>. Accessed: 2016-01-18.

- [3] ebay. <http://www.eBay.com>. Accessed: 2016-08-30.

- [4] Google. <https://developers.google.com/fit/?hl=en>. Accessed: 2016-01-20.

- [5] Health kit constants. [https://developer.apple.com/library/ios/documentation/HealthKit/Reference/HealthKit_Constants/index.html#
//apple_ref/c/tdef/HKBiologicalSex](https://developer.apple.com/library/ios/documentation/HealthKit/Reference/HealthKit_Constants/index.html#//apple_ref/c/tdef/HKBiologicalSex).

- [6] Health kit framework. [https://developer.apple.com/library/ios/documentation/HealthKit/Reference/HealthKit_Framework/index.html#
//apple_ref/doc/uid/TP40014707](https://developer.apple.com/library/ios/documentation/HealthKit/Reference/HealthKit_Framework/index.html#//apple_ref/doc/uid/TP40014707).

- [7] Health kit store.

- [8] National committee on vital and health statistics. privacy and confidentiality in the nationwide health information network, june 2006.
- [9] Personal health information and protection act, 2004. http://www.health.gov.on.ca/en/common/legislation/priv_legislation/. Accessed: 2016-06-27.
- [10] Summary of the hipaa privacy rule. <http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/>. Accessed: 2016-06-27.
- [11] AJZEN, I., AND FISHBEIN, M. Understanding attitudes and predicting social behaviour.
- [12] AL AMEEN, M., LIU, J., AND KWAK, K. Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of medical systems* 36, 1 (2012), 93–101.
- [13] AVANCHA, S., BAXI, A., AND KOTZ, D. Privacy in mobile technology for personal healthcare. *ACM Computing Surveys (CSUR)* 45, 1 (2012), 3.
- [14] BALL, M. J., AND LILLIS, J. E-health: transforming the physician/patient relationship. *International journal of medical informatics* 61, 1 (2001), 1–10.
- [15] BANSAL, G., GEFEN, D., ET AL. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems* 49, 2 (2010), 138–150.

- [16] BARBER, B. *The logic and limits of trust*, vol. 96. Rutgers University Press
New Brunswick, NJ, 1983.
- [17] BATESON, P. The biological evolution of cooperation and trust. *Trust: Making
and breaking cooperative relations, electronic edition. Department of Sociology,
University of Oxford* (2000), 14–30.
- [18] BECKER, M. Y., AND SEWELL, P. Cassandra: Flexible trust management, ap-
plied to electronic health records. In *Computer Security Foundations Workshop,
2004. Proceedings. 17th IEEE* (2004), IEEE, pp. 139–154.
- [19] BÉLANGER, F., AND CROSSLER, R. E. Privacy in the digital age: a review of
information privacy research in information systems. *MIS quarterly* 35, 4 (2011),
1017–1042.
- [20] BLAZE, M., FEIGENBAUM, J., AND LACY, J. Decentralized trust management.
In *Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on* (1996),
IEEE, pp. 164–173.
- [21] BLAZE, M., FEIGENBAUM, J., AND LACY, J. Managing trust in medical
information systems.
- [22] BOK, S. *Lying: Moral choice in public and private life*. Vintage, 2011.
- [23] BOUKERCHE, A., AND REN, Y. A secure mobile healthcare system using trust-
based multicast scheme. *Selected Areas in Communications, IEEE Journal on*
27, 4 (2009), 387–399.

- [24] CHIN, E., FELT, A. P., GREENWOOD, K., AND WAGNER, D. Analyzing inter-application communication in android. In *Proceedings of the 9th international conference on Mobile systems, applications, and services* (2011), ACM, pp. 239–252.
- [25] DEHLING, T., GAO, F., SCHNEIDER, S., AND SUNYAEV, A. Exploring the far side of mobile health: information security and privacy of mobile health apps on ios and android. *JMIR mHealth and uHealth* 3, 1 (2015), e8.
- [26] DEUTSCH, M. Trust and suspicion. *Journal of conflict resolution* (1958), 265–279.
- [27] DEUTSCH, M. Cooperation and trust: Some theoretical notes.
- [28] ER, M. Decision support systems: a summary, problems, and future trends. *Decision support systems* 4, 3 (1988), 355–363.
- [29] ERICKSON, T. From pim to gim: personal information management in group contexts. *Communications of the ACM* 49, 1 (2006), 74–75.
- [30] ESFANDIARI, B., AND CHANDRASEKHARAN, S. On how agents make friends: Mechanisms for trust acquisition. In *Proceedings of the fourth workshop on deception, fraud and trust in agent societies* (2001), vol. 222.
- [31] GALITZ, W. O. *The essential guide to user interface design: an introduction to GUI design principles and techniques*. John Wiley & Sons, 2007.

- [32] GAMBETTA, D., ET AL. Can we trust trust. *Trust: Making and breaking cooperative relations 2000* (2000), 213–237.
- [33] GATES, C., AND WHALEN, T. Private lives: User attitudes towards personal information on the web.
- [34] GEFEN, D., BENBASAT, I., AND PAVLOU, P. A research agenda for trust in online environments. *Journal of Management Information Systems* 24, 4 (2008), 275–286.
- [35] GLAZER, R., AND WEISS, A. M. Marketing in turbulent environments: Decision processes and the time-sensitivity of information. *Journal of Marketing Research* (1993), 509–521.
- [36] GOLEMBIEWSKI, R. T., AND MCCONKIE, M. The centrality of interpersonal trust in group processes. *Theories of group processes 131* (1975), 185.
- [37] HARRINGTON, S. J., AND RUPPEL, C. P. Telecommuting: A test of trust, competing values, and relative advantage. *IEEE Transactions on Professional Communication* 42, 4 (1999), 223–239.
- [38] HART, D. M., ANDERSON, S. D., AND COHEN, P. R. Envelopes as a vehicle for improving the efficiency of plan execution. In *Proceedings of the Workshop on Innovative Approaches to Planning, Scheduling and Control* (1990), Morgan Kaufman, pp. 71–76.

- [39] HAUX, R. Health information systems—past, present, future. *International journal of medical informatics* 75, 3 (2006), 268–281.
- [40] HAUX, R., WINTER, A., AMMENWERTH, E., AND BRIGL, B. *Strategic information management in hospitals: an introduction to hospital information systems*. Springer Science Business Media, 2013.
- [41] HSU, M.-H., JU, T. L., YEN, C.-H., AND CHANG, C.-M. Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations. *International journal of human-computer studies* 65, 2 (2007), 153–169.
- [42] JØSANG, A., ISMAIL, R., AND BOYD, C. A survey of trust and reputation systems for online service provision. *Decision support systems* 43, 2 (2007), 618–644.
- [43] JYDSTRUP, R. A., AND GROSS, M. J. Cost of information handling in hospitals. *Health services research* 1, 3 (1966), 235.
- [44] KÄLLANDER, K., TIBENDERANA, J. K., AKPOGHENETA, O. J., STRACHAN, D. L., HILL, Z., TEN ASBROEK, A. H., CONTEH, L., KIRKWOOD, B. R., AND MEEK, S. R. Mobile health (mhealth) approaches and lessons for increased performance and retention of community health workers in low-and middle-income countries: a review. *Journal of medical Internet research* 15, 1 (2013), e17.

- [45] KETCHPEL, S. P., AND GARCIA-MOLINA, H. Making trust explicit in distributed commerce transactions. In *Distributed Computing Systems, 1996., Proceedings of the 16th International Conference on* (1996), IEEE, pp. 270–281.
- [46] KIM, Y., AND SRIVASTAVA, J. Impact of social influence in e-commerce decision making. In *Proceedings of the ninth international conference on Electronic commerce* (2007), ACM, pp. 293–302.
- [47] KLASNJA, P., AND PRATT, W. Healthcare in the pocket: mapping the space of mobile-phone health interventions. *Journal of biomedical informatics* 45, 1 (2012), 184–198.
- [48] KOTZ, D., AVANCHA, S., AND BAXI, A. A privacy framework for mobile health and home-care systems. In *Proceedings of the first ACM workshop on Security and privacy in medical and home-care systems* (2009), ACM, pp. 1–12.
- [49] LAGENSPETZ, O. Legitimacy and trust. *Philosophical Investigations* 15, 1 (1992), 1–21.
- [50] LUHMANN, N. Trust and power/two works by niklas luhmann; with introduction by gianfranco poggi, 1979.
- [51] LUHMANN, N. Familiarity, confidence, trust: Problems and alternatives. *Trust: Making and breaking cooperative relations* 6 (2000), 94–107.

- [52] LUKOWICZ, P., KIRSTEIN, T., AND TROSTER, G. Wearable systems for health care applications. *Methods of Information in Medicine-Methodik der Information in der Medizin* 43, 3 (2004), 232–238.
- [53] MANDL, K. D., MARKWELL, D., MACDONALD, R., SZOLOVITS, P., AND KOHANE, I. S. Public standards and patients’ control: how to keep electronic medical records accessible but privatemedical information: access and privacydoctrines for developing electronic medical recordsdesirable characteristics of electronic medical recordschallenges and limitations for electronic medical recordsconclusionscommentary: Open approaches to electronic patient recordcommentary: A patient’s viewpoint. *Bmj* 322, 7281 (2001), 283–287.
- [54] MARSH, S., BRIGGS, P., EL-KHATIB, K., ESFANDIARI, B., AND STEWART, J. A. Defining and investigating device comfort. *Information and Media Technologies* 6, 3 (2011), 914–935.
- [55] MARSH, S., WANG, Y., NOËL, S., ROBART, L., AND STEWART, J. Device comfort for mobile health information accessibility. In *Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on* (2013), IEEE, pp. 377–380.
- [56] MARSH, S. P. *Formalising trust as a computational concept*. University of Stirling, 1994.

- [57] MARTÍNEZ-PÉREZ, B., DE LA TORRE-DÍEZ, I., CANDELAS-PLASENCIA, S., AND LÓPEZ-CORONADO, M. Development and evaluation of tools for measuring the quality of experience (qoe) in mhealth applications. *Journal of medical systems* 37, 5 (2013), 1–8.
- [58] MAYER, R. C., DAVIS, J. H., AND SCHOORMAN, F. D. An integrative model of organizational trust. *Academy of management review* 20, 3 (1995), 709–734.
- [59] MCKNIGHT, D. H., AND CHERVANY, N. L. *The Meanings of Trust*. 1996.
- [60] MCKNIGHT, D. H., AND CHERVANY, N. L. What is trust? a conceptual analysis and an interdisciplinary model. *AMCIS 2000 Proceedings* (2000), 382.
- [61] MOJICA, I. J., ADAMS, B., NAGAPPAN, M., DIENST, S., BERGER, T., AND HASSAN, A. E. A large-scale empirical study on software reuse in mobile apps. *IEEE software* 31, 2 (2014), 78–86.
- [62] MUI, L., MOHTASHEMI, M., AND HALBERSTADT, A. A computational model of trust and reputation. In *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on* (2002), IEEE, pp. 2431–2439.
- [63] NARULA, P., DHURANDHER, S. K., MISRA, S., AND WOUNGANG, I. Security in mobile ad-hoc networks using soft encryption and trust-based multi-path routing. *Computer Communications* 31, 4 (2008), 760–769.

- [64] NOWAK, G. J., AND PHELPS, J. Understanding privacy concerns. an assessment of consumers' information-related knowledge and beliefs. *Journal of Direct Marketing* 6, 4 (1992), 28–39.
- [65] OZDALGA, E., OZDALGA, A., AND AHUJA, N. The smartphone in medicine: a review of current and potential use among physicians and students. *Journal of medical Internet research* 14, 5 (2012), e128.
- [66] PAGANO, D., AND MAALEJ, W. User feedback in the appstore: An empirical study. In *2013 21st IEEE international requirements engineering conference (RE)* (2013), IEEE, pp. 125–134.
- [67] PHELPS, J., NOWAK, G., AND FERRELL, E. Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing* 19, 1 (2000), 27–41.
- [68] PODSAKOFF, P. M., MACKENZIE, S. B., LEE, J.-Y., AND PODSAKOFF, N. P. Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology* 88, 5 (2003), 879.
- [69] RAZAVI, M. N., AND IVERSON, L. A grounded theory of information sharing behavior in a personal learning space. In *Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work* (2006), ACM, pp. 459–468.

- [70] RUOHOMAA, S., AND KUTVONEN, L. Trust management survey. In *Trust Management*. Springer, 2005, pp. 77–92.
- [71] SABATER, J., AND SIERRA, C. Review on computational trust and reputation models. *Artificial intelligence review* 24, 1 (2005), 33–60.
- [72] SCHILLO, M., FUNK, P., AND ROVATSOS, M. Using trust for detecting deceitful agents in artificial societies. *Applied Artificial Intelligence* 14, 8 (2000), 825–848.
- [73] SCHULTZ, C. D. A trust framework model for situational contexts. In *Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services* (2006), ACM, p. 50.
- [74] SCOTT, J. *Social network analysis*. Sage, 2012.
- [75] SHAHRIYAR, R., BARI, M. F., KUNDU, G., AHAMED, S. I., AND AKBAR, M. M. Intelligent mobile health monitoring system (imhms). *International Journal of Control and Automation* 2, 3 (2009), 13–28.
- [76] SHERRY, J. M., AND RATZAN, S. C. Measurement and evaluation outcomes for mhealth communication: don’t we have an app for that? *Journal of health communication* 17, sup1 (2012), 1–3.
- [77] SHNEIDERMAN, B. *Designing the user interface*. Pearson Education India, 2003.

- [78] SIAU, K., AND SHEN, Z. Mobile healthcare informatics. *Informatics for Health and Social Care* 31, 2 (2006), 89–99.
- [79] SINHA, R. R., AND SWEARINGEN, K. Comparing recommendations made by online systems and friends. In *DELOS workshop: personalisation and recommender systems in digital libraries* (2001), vol. 106.
- [80] SMITH, S. L., AND MOSIER, J. N. *Guidelines for designing user interface software*. Mitre Corporation Bedford, MA, 1986.
- [81] SONNENBERG, F. A. Health information on the internet: Opportunities and pitfalls. *Archives of internal medicine* 157, 2 (1997), 151–152.
- [82] STONE, E. F., AND STONE, D. L. Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in personnel and human resources management* 8, 3 (1990), 349–411.
- [83] VAWDREY, D. K., HALL, E. S., KNUTSON, C. D., AND ARCHIBALD, J. K. A self-adapting healthcare information infrastructure using mobile computing devices. In *Enterprise Networking and Computing in Healthcare Industry, 2003. Healthcom 2003. Proceedings. 5th International Workshop on* (2003), IEEE, pp. 91–97.
- [84] WANG, P., AND PETRISON, L. A. Direct marketing activities and personal privacy. a consumer survey. *Journal of Direct Marketing* 7, 1 (1993), 7–19.

- [85] WEBSTER, M. Merriam-webster online dictionary.
- [86] WEERASINGHE, D., RAJARAJAN, M., AND RAKOCEVIC, V. Device data protection in mobile healthcare applications. In *Electronic Healthcare*. Springer, 2009, pp. 82–89.
- [87] WEISS, G. M., AND LOCKHART, J. W. The impact of personalization on smartphone-based activity recognition. In *AAAI Workshop on Activity Context Representation: Techniques and Languages* (2012).
- [88] WILHELM, U. G., BUTTYAN, L., AND STAAMANN, S. On the problem of trust in mobile agent systems. In *Symposium on Network and Distributed System Security* (1998), no. LSR-CONF-1998-014, Internet Society.
- [89] XU, H., DINEV, T., SMITH, J., AND HART, P. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems* 12, 12 (2011), 798.
- [90] XU, H., GUPTA, S., ROSSON, M. B., AND CARROLL, J. M. Measuring mobile users’ concerns for information privacy.
- [91] YARMAND, M. H., SARTIPI, K., AND DOWN, D. G. Behavior-based access control for distributed healthcare environment. In *Computer-Based Medical Systems, 2008. CBMS’08. 21st IEEE International Symposium on* (2008), IEEE, pp. 126–131.

- [92] ZACHARIA, G. *Collaborative reputation mechanisms for online communities*. PhD thesis, Massachusetts Institute of Technology, 1999.
- [93] ZHANG, L., AHN, G.-J., AND CHU, B.-T. A role-based delegation framework for healthcare information systems. In *Proceedings of the seventh ACM symposium on Access control models and technologies* (2002), ACM, pp. 125–134.