HAL open science

A Trust-Based Framework for Information Sharing Between Mobile Health Care Applications

Saghar Behrooz, Stephen Marsh

To cite this version:

Saghar Behrooz, Stephen Marsh. A Trust-Based Framework for Information Sharing Between Mobile Health Care Applications. 10th IFIP International Conference on Trust Management (TM), Jul 2016, Darmstadt, Germany. pp.79-95, 10.1007/978-3-319-41354-9_6 . hal-01438350

HAL Id: hal-01438350

https://inria.hal.science/hal-01438350v1

Submitted on 17 Jan 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

A Trust-based Framework for Information Sharing Between Mobile Health care Applications

Saghar Behrooz, Stephen Marsh

Faculty of Business and Information Technology
University of Ontario Institute of Technology, Oshawa, ON, Canada
Saghar.Behrooz@uoit.ca
Stephen.Marsh@uoit.ca

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 paper, 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 for sharing information would be made based on a comparison between the components.
To examine the model, we provide different scenarios. Using mathematical analysis, we illustrate how the model works in those scenarios.

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

1 Introduction

Development of technology has enabled mobile devices as appropriate tools for facilitating health care of various types, in what is known as M-health. M-health provides the opportunity to store and share the health information of a patient in their devices in order to deliver more efficient services, from fitness advice to more physician-oriented tools. However, security of the information in addition to access control is one of the controversial issues in this area [18]. Health care applications collect and share various type of information regarding physical activities and the lifestyles of users in addition to their medical and physiological information [16]. This is a privacy issue that could be better managed.

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" [6].

In 2013 more than 35000 health apps existed for iOS and Android. From the most 600 useful ones, only 183 (30.5%) address mobile health privacy policies in some meaningful way [28]. Recently, both Google and Apple announced new platforms for health apps such as Health Kit [2], Research Kit and Google kit [5], which provide the possibility of information sharing between health care applications in one place.

We consider apple health kit 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 traditional mechanisms such as data encryption. Considering the importance of this information, in addition to usual privacy measurements, other considerations in design need to be met.

To address this, in our current research, we are proposing a trust model which aims to be used as leverage for the owner of the information to 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.

The paper is organized as follows. In section 2 we examine related work, before presenting our proposed model in section 3, and a worked analysis in section 4. We conclude with future work in section 5.

2 Background

In this section, we review existing information systems in the health and M-health area. For the sake of brevity, we look at HealthKit, Apple's health framework in detail. In addition, we provide a summary of current trust-based models and architectures in this area.

2.1 Healthcare Information Systems

Health Information Systems utilize data processing, information and knowledge in order to deliver quality and efficient patient care in health care environments [12]. In recent years, there has been a great deal of movement towards computer-based systems from paper-based systems in health care environments [14]. Computer based systems provide the possibility of patient-centric

systems instead of location constrained systems [7]. Furthermore, targeted users of these systems have also changed. Computer-based systems originally targeted only health care professionals, but gradually they have come to involve patients and their relatives as well [11]. Developments in these information systems over the previous decades provide the possibility of use of data for care planning and clinical research in addition to patient care purposes [11]. In addition, continuous health status monitoring using wearable devices such as sensors and smart watches further enhances the patient experience [17].

Expansions in use of data and health information in parallel with advancements in technology contributed to development of different architectures and information systems in this field. M-health is the use of mobile devices and their information in the health care area [26]. Special characteristics of mobile devices make them an excellent choice for this purpose. Their mobility and ability to access the information in addition to their ubiquity are some of these characteristics [26]. Employing technologies such as text messaging for tracking purposes, cameras for data collection, documentation and their ability to use cellular networks for internet connection, enable mobile devices to act as a perfect platform for delivery of health interventions [15]. Determining exact location through employing positioning technology, is also helpful for emergency situations [26] and device comfort purposes [19], where devices can determine how, when, and where to share relevant health information. 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 device and a communication link between them [29].

One of the major uses of mobile devices in health care is for monitoring purposes. Intelligent mobile health monitoring system (IMHMS) [25], introduces an architecture which is the 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, based on the normal range of the index in question, logically decides whether to send the information to an intelligent medical server or not. The intelligent medical server is monitored by a specialist. Due to the broadness of the field, different monitoring systems have been introduced for specific purposes.

Some architectures have been introduced in order to improve the privacy of health care in this area. Weerasinghe et al [30] present a security capsule with token management architecture in order to have secure transmission and data storage on device. Some models also use access control for healthcare systems based on users behaviours [31]. In [33] the authors propose a role-based prorogate framework. Some architectures have been developed in order to decrease clinical errors. For example, [32] proposes a scenario based diagnosis system which extracts relative clinical information from electronic health records based on the most probable diagnostic hypothesis.

2.2 Information Platform Example: Apple Healthkit

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 [1]. The framework can automatically save data from compatible Bluetooth LE heart rate monitors and the M7 motion coprocessor into the HealthKit store [3].

All the data which 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 [4].

Currently each application is individually responsible for obtaining the trust of the user in order to get access to their health information. The user has the control over the data and can decide whether to share data with the app or not. Users can also share some part of data whilst not giving permission for sharing another part [3].

In order to maintain the privacy of a user's data any application in the HealthKit must have a privacy policy. Personal health records models and HIPAA guidelines can be used in order to create these policies [3].

In addition, data from the HealthKit store cannot be sold. Data can be given to a third party app for medical research with owner consent. The use of data must be disclosed to the user by the application [1].

2.3 Trust in Information Systems

Trust plays an important role in human daily life. Trust can be studied from different perspectives, depending on the person who defines trust and the type of trust [20]. There is wide literature exploring in different fields such as evolutionary biology, sociology, social psychology, economics, history, philosophy and neurology.

The use of Trust Models in electronic healthcare can be classified into two groups: sharing information and electronic health records and monitoring patients. Becker, Moritz and Sewell introduced Cassandra, a trust management system that is flexible in the level of expressiveness 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. The paper concludes with identifying implementation steps including: building a prototype, testing the EHR policy in a more realistic setting, and producing web-based EHR user interfaces [8].

Considering the importance of security in wireless data communication, [9] reviews the characteristics of a secure system and proposes a trust evaluation

model. Data confidentiality, authentication, access control and privacy are examples of mentioned security issues. In this system nodes are representative of each component of system. A trust relationship between nodes has been evaluated to determine trustworthiness of each node. The main difference between this system and related works is that trust value of each node computed based on increased shaped functions such as exponential while others use linear functions. This leads to increase of past behaviour impact on trust [9]. In [21] the authors developed a trust-based algorithm for a messaging system. In this system, each node is assigned a trust value based on their behaviour. At same time, each message was divided to 4 parts and only nodes with the total trust value possible to read all parts of the messages.

3 Our Trust Model

In this section a trust model that considers both personal and environmental aspects is presented. This model aims 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.

To formalize 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 which each person needs for sharing a specific part of the information. 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. In the end, by comparing the two values, advise on sharing the information is made.

Table 1 summarizes the notations used in this chapter:

3.1 Personal Perspective

The personal perspective layer of the model will calculate the amount of trust that the user requires in order to share the information or a specific part of it. This layer is based on 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. Based on personal characteristics and experiences of persons, their behavior varies towards information sharing [13]. Stone and Stone [27] explored links between personality of individuals and information privacy issues. Gefen et al. [10] determined that personality has an impact on trust in virtual environments.

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.

Sensitivity of Information Sensitivity of information might differ for individuals [22–24]. To facilitate the subjectivity of sensitivity of each piece of health

Table 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
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
TR	Threshold for information sharing
T	Trust value

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 calculation of the trust value are the following.

Category of Information: (See table 3.1) Some health information can alter over its lifetime. In our model, we used the Apple health kit categories which falls into two main groups. The first group, "Characteristics data" refers to data which does not change over time such as gender, blood type and date of birth. The second group of data has been collected through the device and might change over time [1, 3].

Table 2. 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).

Purpose of use of information: Different mobile applications use health information for various purposes. Considering existing applications in health care in parallel with the iOS health framework, the aim of use of information categorized to at least one of the several groups.

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:

$$A_i \in P_k \tag{1}$$

in which:

$$k = \begin{cases} Research \\ PersonalMonitoring \\ PublicHealthMonitoring \\ CommercialUsage \\ GovermentalUsage \end{cases}$$

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

We use a matrix in order to represent and determine the relationships between various categories and purposes. 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) value for a specific purpose and category.

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

$$S_{m_p,n_c} = \begin{array}{c} \\ P_1 \\ P_2 \\ \vdots \\ P_{m_p} \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & \cdots & C_{n_c} \end{array} \\ \begin{bmatrix} s_{1,1} & s_{1,2} & \cdots & s_{1,n_c} \\ s_{2,1} & s_{2,2} & \cdots & s_{2,n_c} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m_p,1} & s_{m_p,2} & \cdots & s_{m_p,n_c} \end{bmatrix} \end{array} \tag{2}$$

Through this matrix, the system is able to choose a specific part of information for specific purpose, instead of omitting a whole category of information.

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.

$$\frac{1}{m_p} \sum_{i=1}^{m_p} P_k \tag{3}$$

At this point the trust value for a specific information item in a specific context (application) would be a function of the following variables:

T_d: Delay Time This factor is added in order to improve the privacy of the user. Users can decide on sharing part(s) of their information after a specific delay. This may result in 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:

$$T_d = \begin{cases} 1.5, if \text{ Share immediately} \\ 1, if \text{ Share after one week} \\ 0.5, if \text{ Share after one month} \end{cases} \tag{4}$$

Then:

$$S = f(C, P, T_d) = T_d \cdot \begin{bmatrix} s_{1,1} & s_{1,2} & \cdots & s_{1,n} \\ s_{2,1} & s_{2,2} & \cdots & s_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m,1} & s_{m,2} & \cdots & s_{m,n} \end{bmatrix} \tag{5}$$

3.2 Context Perspective

The second component of the model examines the environment of a user at the time of giving permission for sharing the information. This is used when calculating the amount of trust that exists at any time by considering the following:

- 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 old friend

A higher amount of existing trust results in a lower threshold.

3.3 Default trust to each category and purpose:

Since at the beginning there is no information on the applications, the average trust value which was assigned by the user would be calculated for the sensitivity matrix.

C_0= Default Trust value for all of the categories
P_0= Default Trust value for all of the purposes

$$S_{i_0,j_0} = min(\frac{1}{n_c}\sum_{i=1}^{n_c} C_j, \frac{1}{m_p}\sum_{i=1}^{m_p} P_k) \tag{6}$$

then:

$$S_{m_p,n_c} = \begin{array}{c} \\ P_1 \\ P_2 \\ \vdots \\ P_{m_p} \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & \cdots & C_{n_c} \end{array} \\ \begin{bmatrix} min(C_0,P_0) & min(C_0,P_0) & \cdots & min(C_0,P_0) \\ min(C_0,P_0) & min(C_0,P_0) & \cdots & min(C_0,P_0) \\ \vdots & \vdots & \ddots & \vdots \\ min(C_0,P_0) & min(C_0,P_0) & \cdots & min(C_0,P_0) \end{bmatrix} \end{array} \tag{7}$$

3.4 Application Rating (public social)

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:

$$R_v = \begin{cases} 0.5, if\ v\text{= more than average} \\ 1, if\ v\text{= less than average} \\ 2, if\ v\text{= negative} \end{cases} \tag{8}$$

3.5 Social network friends

Another factor which has impact on the threshold is the number of friends in their social network who are using the application. SN_u represents the number of mutual friends who are using the same application. Considering the number of friends in common SN_u would value one of the followings:

$$SN_u = \begin{cases} 0.5, if\ \text{u= More than 5 friends} \\ 1.5, if\ \text{u= Less than 5 friends} \\ 1, if\ \text{u= No mutual friend} \end{cases} \tag{9}$$

3.6 Installer of the Application:

In health care information systems, the relationship of the person who is asking for the information to the owner of information can have a crucial impact on the existing level of trust between them. Therefore, for example, if a person involved in the patient care suggests an application, the application in question is seen as potentially more reliable. In this model, 3 scenarios have been 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:

$$I_t = \begin{cases} 0.5, if\ \text{t=Healthcare provider suggests} \\ 0.75, if\ \text{t=Proposed by a sensor the user already uses} \\ 1, if\ \text{t= Randomly downloaded application} \end{cases} \tag{10}$$

3.7 Estimation of the Threshold

Considering all the factors the second component of the model would be:

$$TR = S_0 \cdot R_v \cdot SN_u \cdot I_t \tag{11}$$

Information would be shared if :

$$TR < T \tag{12}$$

4 Analysis

In this part, we examine our model using different scenarios as use case examples. Furthermore, different user personalities and various applications have been considered.

4.1 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 section each category is described:

Optimist An optimist believes in the best outcome in all the situations and expects the best results in everything [20]. In our examples, an optimist always selects the maximum trust value.

Pessimist In the eyes of pessimist, in opposite to the optimist, the worst possible result is being seen. The pessimist expects the worst outcome in any situation. Therefore, the pessimist agent selects the worst trust value in all the situations [20].

Realist However, in reality most people are some place between the two extremes. This situation also applies 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 pessimist

4.2 Pool of Applications

In healthcare environments, various applications with different characteristics exist. This section looks at examples of these applications.

Application $\boldsymbol{\alpha}$ 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.

Application $\boldsymbol{\beta}$ Application β has the following characteristics:

- This app 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.

4.3 Various Situations

Although personality plays a significant role in decision making other factors including the experiences of the user or their current mental state can affect their judgment. To address this, we test the model in 2 different scenarios.

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 is using this application. This application needs to have access to her fitness information, nutrition information and weight information.

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. In order to monitor himself he decides to install an sleep analysis application on his device.

4.4 Mathematical Analysis

In order to examine how the model works, in this part we briefly analyse the model in different situations.

Example 1. In the first scenario, we consider Tracy as an optimist. Therefore, she relatively assigns a higher trust value for sharing information. Table 3 represents the trust values she assigned for each purpose and category.

Table 3. 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	Govermental usage	0.73

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

and purpose, therefore:

$$S = f(C, P) = \begin{bmatrix} 0.22 & 0.22 & 0.22 & 0.22 & 0.22 \\ 0.31 & 0.31 & 0.31 & 0.22 & 0.31 \\ 0.46 & 0.32 & 0.46 & 0.22 & 0.33 \\ 0.51 & 0.32 & 0.46 & 0.22 & 0.33 \\ 0.73 & 0.32 & 0.46 & 0.22 & 0.33 \end{bmatrix} \tag{13}$$

$$t_d = 1.5 \tag{14}$$

Then the trust matrix would be:

$$S_{m,n} = \begin{array}{c} \\ Research \\ PersonalMonitoring \\ PublicHealth \\ CommercialUsage \\ GovernmentalUsage \end{array} \begin{array}{c} \begin{array}{ccccc} VitalSigns & SleepAnalysis & Dobymeasurements & Fitness & Nutrition \end{array} \\ \begin{bmatrix} 0.33 & 0.33 & 0.33 & 0.33 & 0.33 \\ 0.46 & 0.46 & 0.46 & 0.33 & 0.46 \\ 0.69 & 0.48 & 0.69 & 0.33 & 0.49 \\ 0.76 & 0.48 & 0.69 & 0.33 & 0.49 \\ 1.09 & 0.48 & 0.69 & 0.33 & 0.49 \end{bmatrix} \end{array} \tag{15}$$

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

$$S_{i_0,j_0} = min(\frac{1}{5}\sum_{i=1}^{5} C_j, \frac{1}{5}\sum_{i=1}^{5} P_k) = min(0.428, 0.444) = 0.428 \tag{16}$$

$$S = f(C, P) = \begin{bmatrix} 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \\ 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \\ 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \\ 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \\ 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \end{bmatrix} \tag{17}$$

And:

$$R_v = 1 \tag{18}$$

$$SN_u = 1 \tag{19}$$

$$I_t = 1 \tag{20}$$

The the threshold matrix would be:

$$TR = \begin{bmatrix} 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \\ 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \\ 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \\ 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \\ 0.428 & 0.428 & 0.428 & 0.428 & 0.428 \end{bmatrix} \tag{21}$$

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 wont 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 those information, trust value is higher than the threshold.

$$0.33 < 0.428 \rightarrow Do\ not\ share \tag{22}$$

$$0.46 > 0.428 \rightarrow Share\ vital\ signs\ information\ for\ personal\ monitoring \tag{23}$$

Example 2 In the second scenario, we considered Steve as a pessimist. He does not give high trust values to the application. Therefore he assigns the following trust values as noted in table 4.

Table 4. 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	Govermental usage	-0.59

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

$$S = f(C, P) = \begin{bmatrix} -0.31 & -0.68 & -0.22 & -0.46 & -0.33 \\ -0.31 & -0.68 & 0.11 & -0.46 & -0.33 \\ -0.47 & -0.68 & -0.47 & -0.47 & -0.47 \\ -0.86 & -0.86 & -0.86 & -0.86 & -0.86 \\ -0.59 & -0.68 & -0.59 & -0.59 & -0.59 \end{bmatrix} \tag{24}$$

Steve decides to share his information after one week.

$$t_d = 1 \tag{25}$$

Then the trust matrix would be:

$$S_{m,n} = \begin{array}{c} \\ Research \\ PersonalMonitoring \\ PublicHealth \\ CommercialUsage \\ GovernmentalUsage \end{array} \begin{array}{c} \begin{array}{ccccc} VitalSigns & SleepAnalysis & Bodymeasurements & Fitness & Nutrition \end{array} \\ \begin{bmatrix} -0.31 & -0.68 & -0.22 & -0.46 & -0.33 \\ -0.31 & -0.68 & 0.11 & -0.46 & -0.33 \\ -0.47 & -0.68 & -0.47 & -0.47 & -0.47 \\ -0.86 & -0.86 & -0.86 & -0.86 & -0.86 \\ -0.59 & -0.68 & -0.59 & -0.59 & -0.59 \end{bmatrix} \end{array} \tag{26}$$

We consider that that application β is the application which Steve has installed. Therefore, we have:

$$S_{i_0,j_0} = min(\frac{1}{5}\sum_{i=1}^{5} C_j, \frac{1}{5}\sum_{i=1}^{5} P_k) = min(-0.31, -0.406) = -0.406 \tag{27}$$

$$S = f(C, P) = \begin{bmatrix} -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \\ -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \\ -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \\ -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \\ -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \end{bmatrix} \tag{28}$$

And:

$$R_v = 1 \tag{29}$$

$$SN_u = 1 \tag{30}$$

$$I_t = 1 \tag{31}$$

The the threshold matrix would be:

$$TR = \begin{bmatrix} -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \\ -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \\ -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \\ -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \\ -0.406 & -0.406 & -0.406 & -0.406 & -0.406 \end{bmatrix} \tag{32}$$

Again, by comparing matrix elements, a recommended decision for information sharing can be made. In this case, sleep analysis information won't be shared. Also, nutrition information wont be shared as application β use this information for public health purposes.

$$-0.68 < -0.406 \rightarrow \textit{Do not share} \tag{33}$$

$$-0.33 > -0.406 \rightarrow \textit{Share nutrition information for research} \tag{34}$$

$$-0.33 > -0.406 \rightarrow \textit{Share nutrition information for personal monitoring} \tag{35}$$

$$-0.47 < -0.406 \rightarrow \textit{Do not share nutrition information} \tag{36}$$

5 Conclusions and Further Work

In this paper, we proposed a trust model which calculates the required trust value of information sharing between health care mobile applications, in addition 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. Moreover, by categorizing the information and purpose of use, we aim to provide provide the opportunity for sharing in different levels. Going forward, we plan to implement the framework and the corresponding user interfaces, and a user study is in the planning stage.

6 Acknowledgment

The authors gratefully acknowledge the support of the Natural Sciences and Engineering Research Council of Canada under the Discovery Program.

References

1. Apple inc, https://developer.apple.com/library/ios/documentation/UserExperience /Conceptual/MobileHIG/HealthKit.html
2. Apple inc. health kit, https://developer.apple.com/healthkit
3. Apple inc, the health kit framework, https://developer.apple.com/library/ios /documentation/HealthKit/Reference/HealthKit_Framework/
4. Apple inc, the health kit framework, https://developer.apple.com/library/ios /documentation/HealthKit/Reference/HKHealthStore_Class/index.html#//apple_ref /occ/cl/HKHealthStore
5. Google, https://developers.google.com/fit/?hl=en
6. National committee on vital and health statistics. privacy and confidentiality in the nationwide health information network, june 2006, http://www.ncvhs.hhs.gov/060622lt.html
7. Ball, M.J., Lillis, J.: E-health: transforming the physician/patient relationship. International journal of medical informatics 61(1), 1–10 (2001)
8. Becker, M.Y., Sewell, P.: Cassandra: Flexible trust management, applied to electronic health records. In: Computer Security Foundations Workshop, 2004. Proceedings. 17th IEEE. pp. 139–154. IEEE (2004)
9. Boukerche, A., Ren, Y.: A secure mobile healthcare system using trust-based multicast scheme. Selected Areas in Communications, IEEE Journal on 27(4), 387–399 (2009)
10. Gefen, D., Benbasat, I., Pavlou, P.: A research agenda for trust in online environments. Journal of Management Information Systems 24(4), 275–286 (2008)
11. Haux, R.: Health information systems–past, present, future. International journal of medical informatics 75(3), 268–281 (2006)
12. Haux, R., Winter, A., Ammenwerth, E., Brigl, B.: Strategic information management in hospitals: an introduction to hospital information systems. Springer Science Business Media (2013)
13. Hsu, M.H., Ju, T.L., Yen, C.H., 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), 153–169 (2007)
14. Jydstrup, R.A., Gross, M.J.: Cost of information handling in hospitals. Health services research 1(3), 235 (1966)
15. Klasnja, P., Pratt, W.: Healthcare in the pocket: mapping the space of mobile-phone health interventions. Journal of biomedical informatics 45(1), 184–198 (2012)
16. Kotz, D., Avancha, S., 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. pp. 1–12. ACM (2009)
17. Lukowicz, P., Kirstein, T., Troster, G.: Wearable systems for health care applications. Methods of Information in Medicine-Methodik der Information in der Medizin 43(3), 232–238 (2004)
18. Mandl, K.D., Markwell, D., MacDonald, R., Szolovits, P., 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 recordscommentary: A patient's viewpoint. Bmj 322(7281), 283–287 (2001)

19. Marsh, S., Wang, Y., Noël, S., Robart, L., Stewart, J.: Device comfort for mobile health information accessibility. In: Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on. pp. 377–380. IEEE (2013)
20. Marsh, S.P.: Formalising Trust as a computational concept. Ph.D. thesis
21. Narula, P., Dhurandher, S.K., Misra, S., Woungang, I.: Security in mobile adhoc networks using soft encryption and trust-based multi-path routing. Computer Communications 31(4), 760–769 (2008)
22. Nowak, G.J., Phelps, J.: Understanding privacy concerns. an assessment of consumers' information-related knowledge and beliefs. Journal of Direct Marketing 6(4), 28–39 (1992)
23. Phelps, J., Nowak, G., Ferrell, E.: Privacy concerns and consumer willingness to provide personal information. Journal of Public Policy & Marketing 19(1), 27–41 (2000)
24. Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y., Podsakoff, N.P.: Common method biases in behavioral research: a critical review of the literature and recommended remedies. Journal of applied psychology 88(5), 879 (2003)
25. Shahriyar, R., Bari, M.F., Kundu, G., Ahamed, S.I., Akbar, M.M.: Intelligent mobile health monitoring system (imhms). International Journal of Control and Automation 2(3), 13–28 (2009)
26. Siau, K., Shen, Z.: Mobile healthcare informatics. Informatics for Health and Social Care 31(2), 89–99 (2006)
27. Stone, E.F., Stone, D.L.: Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. Research in personnel and human resources management 8(3), 349–411 (1990)
28. Sunyaev, A., Dehling, T., Taylor, P.L., Mandl, K.D.: Availability and quality of mobile health app privacy policies. Journal of the American Medical Informatics Association 22(e1), e28–e33 (2015)
29. Vawdrey, D.K., Hall, E.S., Knutson, C.D., 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. pp. 91–97. IEEE (2003)
30. Weerasinghe, D., Rajarajan, M., Rakocevic, V.: Device data protection in mobile healthcare applications. In: Electronic Healthcare, pp. 82–89. Springer (2009)
31. Yarmand, M.H., Sartipi, K., Down, D.G.: Behavior-based access control for distributed healthcare environment. In: Computer-Based Medical Systems, 2008. CBMS'08. 21st IEEE International Symposium on. pp. 126–131. IEEE (2008)
32. Yousefi, A., Mastouri, N., Sartipi, K.: Scenario-oriented information extraction from electronic health records. In: Computer-Based Medical Systems, 2009. CBMS 2009. 22nd IEEE International Symposium on. pp. 1–5. IEEE (2009)
33. Zhang, L., Ahn, G.J., 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. pp. 125–134. ACM (2002)