A Patient-Centric Approach for Intelligent Privacy Policies Generation in Mobile Healthcare

Souad Sadki[1], Hanan El Bakkali[2]
Mohammed V-Souissi University
National School Of Computer Science And Systems Analysis[1,2]
Rabat, Morocco

Abstract

Mobile technologies are changing the way patients are receiving care services. Thanks to mobile devices such as smartphones, tablets and patient monitoring devices, patients are integrated in managing their own health, real time patient information is easily provided to physicians and patient-physician communication becomes easier. Nevertheless, although mobile healthcare offers many benefits, there is also a downside to using these mobile technologies. Privacy is among the primary issues to address. In fact, patients become more and more concerned about "what happen" to their data while being exchanged with third parties. In this paper, we focus on privacy concerns in mobile healthcare. We introduce an approach to preserve patients' privacy in Mobile Healthcare named PPIAMH. This solution aims to get patients involved in defining their privacy preferences regarding the disclosure of their sensitive medical information based on an intelligent mobile application and access control mechanisms. Different aspects of our solution are illustrated by a real world scenario that evinces how patients' privacy policies are defined using the suggested approach.

1. Introduction

Technological innovation is transforming the way users and service providers communicate. Nowadays, mobile technologies such as smartphones are not only the key computing and communication mobile devices, but an ensemble of embedded sensors that collectively enable new applications in various areas like homecare, healthcare, social networks, safety, environmental monitoring, e-commerce and transportation [1].

Today in healthcare systems, the utilization of mobile devices is becoming more and more frequent. Indeed, mobile technology is helping with chronic disease management, empowering the elderly and expectant mothers, reminding people to take medication at the proper time, extending service to underserved areas, and improving health outcomes and medical system efficiency [2].

Traditionally, patients' health information records were created with paper and kept in storing boxes.

Nowadays, with the speed evolution of Information and Communication Technologies (ICT), medical data is recorded electronically in storing files in computer servers that can be located anywhere. Particularly, with the emergence of Cloud computing services, electronic medical records can be stored via the internet in remote servers. This may increases privacy breaches since the Cloud infrastructure is shared between multiple tenants. As a result, users become "anxious" of their private information when they are uncertain who may gain access to their personal data after being uploaded to the server and how it will be used or shared [3].

In this article, we propose a privacy-preserving approach for mobile healthcare which aims to integrate patient's privacy preferences regarding the divulgation of their health information during a mobile transaction. In other words, we try to make patient's privacy policies considered next to healthcare and Cloud providers privacy policies. More impressively, our solution's main objective is to predict patient's preferences through a usable and a simple way since patients are not often able to make decisions or read complex privacy policies that their healthcare providers impose. These policies must be expressed and presented in a comprehensive way in order to prevent any kind of conflict.

Also, since multiple actors are involved in patients' care, it becomes a must to restrict access to patients' private data. For this purpose, above formal privacy and security policies definition, efficient access control mechanisms such as attributes based access control (ABAC) are needed to prevent unauthorized usage or disclosure of data.

The paper is structured as follows: Section 2 presents a background on privacy and mobile healthcare followed by related works presentation in Section 3. Next, we introduce in Section 4 the notion of privacy group. The main components and steps of our proposed solution is presented in Section 5 followed by a real world scenario that evinces how patients can participate in defining the privacy policies reinforced by access control mechanisms. Section 6 concludes the paper with future works.

2. Privacy in Mobile Healthcare

2.1. Mobile Healthcare evolution

The massive usage of mobile technologies in different contexts has improved individual's quality of life. As for the health sector, mobile technologies ensure a highest quality of care for patients making physician-patient communication easier and more flexible. More importantly, patients are integrated in managing their own health through mobile web-based applications. Also, patients with chronic disease such as diabetes or high blood pressure can send medical reports and test results to their doctors. That way, they avoid the long waiting time in doctor's office or hospitals.

Mobile technologies do not only facilitate the exchange of data between patients and physicians, it also allows physicians to communicate with health professionals all over the world.

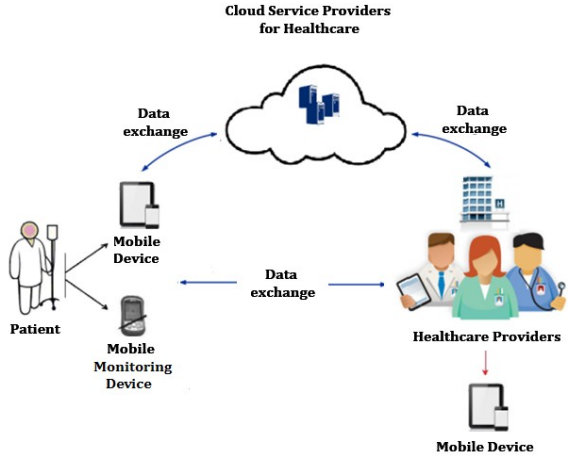


Figure 1. Main actors in a mobile healthcare system [4]

As shown in Figure 1, three main actors are involved in a mobile healthcare system: the Patient, Healthcare Providers and Cloud Services Providers [4]. Remarkably, the multiplicity of actors involved in patients care makes patients more and more concerned about "what happen" to their data while being exchanged.

2.2. Mobile Healthcare and privacy concerns

Privacy is a primary matter in individuals' life especially for patients. It has a significant impact on patients' outcomes particularly for patients suffering from serious diseases.

The usage of mobile technologies in healthcare provides new privacy concerns. On one hand, the emergence of Cloud services has facilitated the management and storage of information but also caused new privacy breaches. One the other hand, Mobile devices such as Smartphone or tablet is not only used in the health context but for many other purposes such as searching in the internet, connecting with people by means of social networks and so on. Hence, new privacy concerns can take place putting patients' sensitive data at risk. Thus, efficient measures are needed to preserve privacy and include patient in protecting their data by respecting their preferences concerning the usage and disclosure of their medical information.

2.3. Privacy policies in mobile healthcare

In order to protect patients' sensitive data from possible misusing or disclosure, healthcare providers and organizations should have a clear understanding of data sources and the privacy requirements that follow this data [7]. Thus, privacy requirements and policies must be formalized and presented in a comprehensive way to prevent any kind of conflicts since privacy policies are not necessary similar. An interesting example of such conflict was presented in [7]. Faccebook, Zynga and AOL Advertising are given as examples of parties whose privacy policies are different. The Facebook policy prohibits the transfer of any data to advertisers, regardless of whether users consent to the transfer [7]. The same goes with Zinga privacy policy which prohibits such transfers without users' consents [7] while AOL Advertising (the advertiser) retains the right to use collected information.

As for the healthcare sector, conflicts between healthcare providers' may occur due the differences in privacy policies. In [8], a concrete example is given describing a patient in a critical condition (emergency) and where access to his medical data is confusing. Two examples of privacy policies are given; one allowing access to data in urgent situation and the other restrict access to the psychiatrist only. On one hand, the patient may be in danger if access to his data is denied (if he's allergic to anesthesia for example) and his sensitive data may be disclosed without his consent on the other hand [8].The same situation could occur with a doctor using his mobile device to ask others health professionals' opinions concerning an accurate health condition. So, efficient tools are needed to ensure consistency between privacy requirements across different parties [7].

3. Related Works

We classify the research works into three main categories. The first category is interested in preserving patients' privacy in mobile healthcare. The second one tries to improve patients' quality of care through mobile intelligent solutions. Finally, the

third category focuses on privacy policies formulation and presentation.

Concerning the first category, a series of recent privacy-preserving solutions have been proposed in the literature. Most of which deploy access control mechanisms to preserve privacy. Exemplary, we cite an Opportunistic (OC) Computing framework for healthcare emergency presented in [13]. This solution aims to achieve user-centric privacy access control by allowing a medical user to decide who can participate in the OC [13]. Second, a conceptual privacy framework has been suggested in [14]. According to this proposition, individuals need to be provided by opportunities to make informed decisions about the collection, use, and disclosure of their health data [14]. The same authors suggest in [15] a privacy framework for mobile healthcare and home-care systems. By setting a number of privacy properties, this solution serves as a guide for developers and searchers for building more effective privacy preserving solutions.

Another category of researchers are interested in developing intelligent solutions aiming to improve patients' quality of care. In this regard, an intelligent telecardiology system has been proposed in [16] which help patients for cardiovascular disease diagnosis and treatment in mobile platforms [16]. Also, authors in [17] developed a mobile intelligent system for eye examination. This solution deployed in mobile smartphones mainly help patients with diabetes from blindness by identifying retinal diseases conditions. In the same context, a Cloud-based intelligent solution has been presented in [18] allowing real time monitoring of chronic diseases such as diabetes.

Thanks to its crucial role in protecting patients' sensitive data from unauthorized usage or disclosure, privacy policies have been the main study object of a number of recent researches [8-19-20]. Some of these studies consider the importance of expressing these policies in a formal and comprehensive way.

We try to incorporate the intelligence characteristic in our solution to fulfill patients' need in an easy way. On another line, we aim to involve him in expressing his privacy preferences that our solution will "translate" in adequate privacy policies.

4. Patients' preferences classification

4.1. Privacy groups

We refer to Westin's classification [9] to distinguish patients' in terms of privacy preferences. According to this classification, patients can be divided into three main groups: the Fundamentalist, the Pragmatic and the Unconcerned group.

Since patients are not always in a condition that allows them to make decisions regarding their privacy preferences (children, elderly, patients badly hurt..), we define a new group called: the "*Should-Be-Protected*" group.

i. The Fundamentalist group:

Patients that distrust healthcare organizations or Cloud providers to protect their privacy, they prefer to control access to their data and are in favor of new laws and regulatory actions to clarify privacy rights and provide enforceable remedied [10].

ii. The Pragmatic group:

Patients who ponder the benefits of protection and regulation next to the amount of data they are prepared to divulgate [11]. They want the opportunity to decide whether they trust organizations or ask for legal procedures to protect their personal information [10].

iii. The Unconcerned group:

Patients that trust health organizations or any third party to protect their private data. They are comfortable with the existing organizational procedures [10].

For the third category, we define an educational zone (privacy awareness) allowing patients to be informed of the different actions/risks that may endanger the safety of their data. The main objective of this zone is to make unconcerned patients change their point of view towards his privacy.

iv. The Should-Be-Protected group:

In this group, the patient does not actually belongs to the "Unconcerned" group; at the same time he can't take decisions or make preferences regarding the disclosure of his private medical data. Therefore, he is automatically classified as "Should-Be-Protected" patient. This group includes children that can't take proper decision and need a guardian, patient badly hurt (patients in the hospital) or patients with critical mental condition.

4.2. Privacy levels

In order to facilitate patients' privacy policies generation, we assign a privacy level for each privacy group defined in the previous section. These levels serve as key indicators that characterize each privacy group.

We refer to [12] for privacy level nomination, namely, privacy level 1 for the Fundamentalist group (PL-1) [12], privacy level 2 for the Pragmatic group (PL-2) [12], privacy level 3 for the Unconcerned group (PL-3) [12]. We add a new privacy level for the new group (PL-D) which is the default level automatically activated if none of the three previous levels is selected.

i. PL-1 level:

This level corresponds to the fundamentalist group, for this level the patient doesn't trust any organizations and prefer a full control of his sensitive information.

However, even if he doesn't allow the sharing of his information with others (for instance a non

medical person or other physicians not involved in his treatment), a fundamentalist patient may want to share some of his information with patient having similar assumptions or professionals physicians that can give extra interpretations about his health condition.

ii. PL-2 level:

This level corresponds to the pragmatic and the "Should-Be-Protected" group. Concerning the pragmatic group who believes that trust should not be freely given but earned and seek for options [11]. For this level, the patient is given the flexibility to decide who has access to what and under what condition.

iii. PL-3 level:

We believe that even a patient is unconcerned, his privacy must be protected. That's why an educational zone was introduced to make him aware of the risks that endanger his privacy while using a mobile device. In fact, mobile devices like smartphones are not only used in health context.

iv. PL-D level (Default):

For the "Should-Be-Protected" group who can be a fundamentalist, a pragmatic or an unconcerned group but can't make decisions, the protection of sensitive data is ensured by preventing a total disclosure. In this case, a default configuration is performed.

5. The proposed privacy-preserving approach

5.1. Motivations

This solution is a part of our previous work entitled Privacy Module for Mobile Healthcare that aims to: 1) Protect data collected, transferred and stored, 2) Make patient an active actor regarding data disclosure and usage authorizations, and 3) Take into account Cloud-computing issues [4]. In this article, we focus on the second objective which is considering patients' decision concerning the divulgation of their private data (to whom, for what reason). Therefore, we suggest a Privacy-Preserving Approach for Mobile Healthcare (PPAMH). This solution gives patients (mobile users) the opportunity to exercise as much control as desired over disclosure [11] while predicting patients' behavior/preferences over the usage of their mobile data. Our main concern is to design a usable solution which helps patients to make preferences and make decisions knowing that patients can't deal with complex privacy policies.

5.2. PPAMH architecture:

In this section, we present the general architecture of our solution. It consists of the following components:

i. Privacy-Preserving Intelligent Application:

The Privacy-Preserving Intelligent Application for Mobile Healthcare (PPIAMH) is an intelligent mobile application which has two main tasks (Modules):

- Determine the group type (Fundamentalist, Pragmatic, Unconcerned or Should-be-Protected): The group is designated through a simple questionnaire that patient should fulfill. (if his health condition allows his to do so).
- Predict patient's privacy preferences concerning the attributes he wants to divulgate or not and to whom these attributes can be disclosed.

ii. Trusted third party:

A trusted authority whose main objectives are:

- "Transform" patients' preferences into formal privacy policies.
- Provides an agreement that must be approved by Healthcare and Cloud providers.

iii. An agreement:

This agreement is settled between the trusted third party and Healthcare/Cloud providers. It obliges them to respect patient preferences and other parties' privacy policies to prevent any kind of conflict.

5.3. Privacy policies assignment process

In order to assign the adequate privacy policies to the right patient, three main steps are performed. In **Phase 1,** the group to which the patient belongs is defined. Next, in **Phase 2**, patients' privacy preferences are determined according to the group he belongs to. These preferences are presented by a set of rules. These rules are sent to the trusted third party to generate the correspondent privacy policies (**Phase 3**).

i. Group determination

The PPIAMH intelligent application provides patients (in a good condition) with a simple questionnaire. Patients are asked to answer simple ordinary questions. We take into consideration that patients' educational levels, ages and conditions are different that's why questions should be as simple as possible. For this purpose, we refer to a survey on privacy-related issues of Canadians citizens [6].We picked up three relevant questions that can be addressed to mobile patient to figure out whether he is a fundamentalist, pragmatic or unconcerned.

- ***Question 1****:* In general, how concerned are you about the protection of your privacy? Very concerned, concerned or not concerned. [6]
- ***Question 2****:* Do you usually share your personal information with organizations that ask for it? Would you say you do this never, rarely, sometimes, often or always? [6]

- ***Question 3:*** If the personal information you have given to an organization is lost, stolen or unintentionally exposed, do you think that organization would notify you? [6]

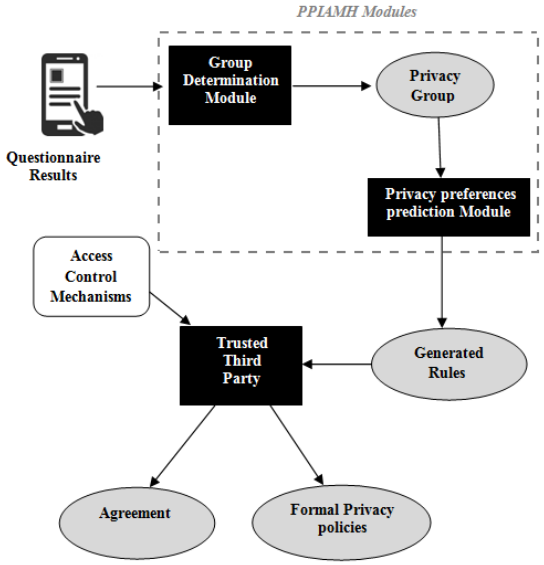


Figure 2. Process of the proposed approach

As described in Figure 2, the group determination module determines the privacy group according to patients' answers. Then, the Privacy preferences prediction module generates a set of rules that will be translated to formal privacy policies by the trusted third party. It finally settle an agreement with third parties so as they approve and respect patients' preferences.

Let MP= {mp_1, mp_2, mp_3 …. mp_n} denote N patients using mobile devices or whose data can be used by a mobile user (Doctor, Nurse...). As shown is Figure. 3, a patient can belong to the Fundamentalist **(F)**, the Unconcerned (**U**), the Pragmatic (**P**) or to the Should-Be-Protected (**SP**) group depending on his answers to the questionnaire (Score). An awareness zone is dedicated to the unconcerned patients to highlight and present the different privacy risks that may occur when using mobile devices.

We define two Boolean variables Q, Aw representing respectively the questionnaire and privacy awareness functionalities.

When a patient answers the questionnaire, **Q** is set to 1 and set to 0 otherwise. When the privacy awareness functionality is activated, then **Aw** is set to 1. Also, we define **S** the score of the patient who could answer the questionnaire. **NS** is the score obtained after activating the awareness zone.

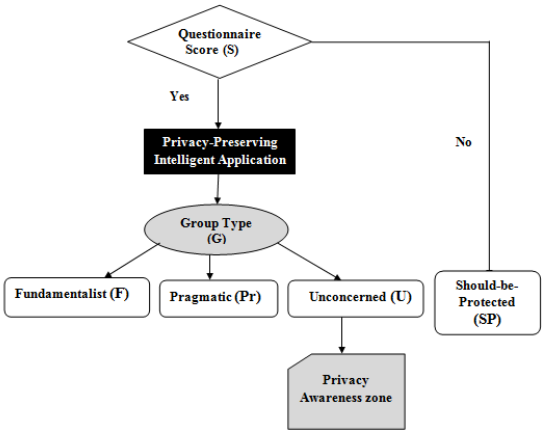


Figure 3. Privacy group determination Process

The group determination algorithm is defined as follows:

Algorithm Group type determination

Input : **S** patient Score
Output: **G** privacy group type where G ∈{F; P; U; SP}

1. We define **the three following variables**:
   T: threshold for Fundamentalist
   Tu: threshold for Unconcerned
   Tw: privacy awareness threshold
2. **for** each $mp_i \in$MP
3. **if** (**Q**=1) **then**

DetGroup:

4. **if (S>=T)then**
5. **G**="F"
6. **else** // the patient can choose to trust third parties or is unconcerned
7. **if(S>= Tu) then G**="P"
8. **else**
   G="U"
9. **endif**
10. **Endif**
11.
12. **if(G**="U") // if the patient is unconcerned
13. **Aw**=1 //privacy awareness activation
14. **N=NS +N**
    Go DetGroup
    Endif
15. **Else** // Q=0; // the patient couldn't answer the questions
16. **U="**SP"
17. **Endif**
18. **Return** G
19. **End**

If the questionnaire option **Q** is activated, the intelligent mobile application determines the privacy group using the Score value (**S**). The two variables **T** (Fundamentalist), **Tu** (Unconcerned) are used for this purpose. If the patient belongs to the "Unconcerned" group **(G="U")**, then the option **Aw** is activated providing patient with an awareness

zone. Therefore, the score are recalculated **(SN),** it can be changed (if the patient is convinced) or remain the same if the patient does not change his mind.

If the questionnaire option **Q** is deactivated (patients couldn't answer the questionnaire), then the patient is automatically classified as a "Should-Be-Protected" patient.

v. Privacy preferences prediction

After specifying the privacy group to which the patient belongs, the next steps aims to predict his privacy preferences (which attributes to disclose, to whom) and also the purpose of data usage. For each group we rely on the privacy level defined in Section 4. Each level is associated with a group type.

vi. Rules generation

After predicting patients' privacy preferences, a set of formal rules is generated defining the entities permitted to access patients' data and the actions performed to that data. Notably, the major particularity of these rules is that they incorporate privacy preserving aspects. In order to facilitate rules generation and then privacy policies expression we consider the two basic elements *Subject* and *Object* and their attributes where "Subject" designates a user willing to grant access to a protected resource [5].Object is the resource protected [5]. For each subject or object we assign a set of "Attributes" or characteristics. An example of subject is "Cloud provider" having the two attributes "deployment model type" and "service model type". An example of object is "medical history" with the two attributes "date of creation" and "size".

vii. Agreement settlement

The trusted third party set an agreement addressed to third parties including Healthcare and Cloud providers. The objective of this agreement is to make third parties consider patient's preferences.

viii. Formal privacy policies generation

The trusted third party relies on the privacy preferences rules defined in the previous section to create formal privacy policies. These policies should be standardized and presented in a simple manner to be understood by different third parties. For this purpose, XACML (eXtensible Access Control Markup Language) can be used as a tool for privacy policies description.

Notably, protecting patients' privacy requires controlling access to their sensitive data. For this purpose, sophisticated access control models such as attribute based access control are needed. In this regard, an interesting extended attribute based access control (ABAC) model for collaborative environment was suggested in [5].

In fact, the existing ABAC models consider only the subjects, the resources and the actions to perform whereas the extended model suggested in [5] takes into account the entities' *attributes*, the general *context* as well as the *purpose* of the requests [5].

More interestingly, it incorporates trust and privacy issues. Thus, this model can be applied in healthcare environments since multiple collaborative healthcare systems and organizations are involved in patients' care.

5.4. Overview of the extended ABAC model with Trust and Privacy

i. Basic components

According to the model definitions suggested in [5], the main components and their representation are described as follows:

- **Subject:** User who want to grant access to the resource. It is represented by **"s".**
- **Object**: The resource protected, represented by **"o".**
- **Attributes**: Characteristic of the entity. A set of attributes is represented by **"ATTR".**
- **Operations**: Actions that can be applied to the object. A set of operations is represented by **"OP"** (read, write…).
- **Permissions:** authorization assigned to objects. An operation set is represented by **"PERM'** (allow, deny…).
- **Contexts:** circumstances under which the access occur [5].The contexts for this model are presented by **"CTXT"**
- **Permission assignment functions:** The functions used to apply access control policies. They are represented by **pa_i()** where **"i"** indicates an accurate policy rule.

ii. Trust et privacy incorporation

As mentioned before, the main particularity of this model is that it takes into consideration trust and privacy issues.

- **Trust:** for each subject we assign a trust level as one of its attributes represented by the value '**Ptr(s)'** where $0 \leqslant \text{Ptr(s)} \leqslant 1$, with 0 indicates that the subject is totally untrustable and 1 for a totally trusted subject [5]
- **Privacy:** the notion of *well-defined purpose* is utilized to express the reason for which the subject wants to gain access to data [5**].**
  A purpose assignment function is defined represented by **"purp_assign".** It returns the attribute of purposes set to a subject [5].

iii. Application of the model to our solution

As previously mentioned, the elements Objects, subjects and their attributes [5] are used as key components to facilitate formal privacy policies expression. The extended attribute based access control described here is considered as an efficient access tool on which the trusted third party can rely to define the different access rules according the formal privacy policies generated. Mainly, we focus on the privacy preserving aspect of this model.

Figure 5 shows how this model is incorporated into our solution to preserve patients' privacy.

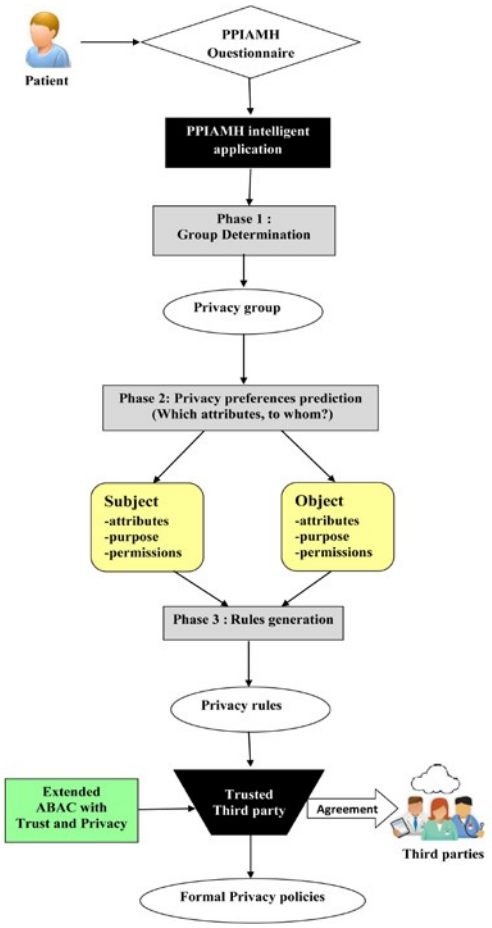


Figure. 5 PPAMH with the extended ABAC model

As shown in Figure 5, the objects, subjects and associated attributes as well as the permissions assigned are determined by the privacy preferences prediction module to prepare for the rules generation. These rules are then used by the trusted party that relies on the ABAC model to generate the associated access control rules.

5.5. Case study

In this section we provide an example of scenario that shows how privacy preferences can be predicted and transformed into defined privacy rules.

For this purpose we will use the notation presented in the previous sections to facilitate privacy rules as well as formal privacy policies generated by the trusted party. Also, as mentioned before, preserving patients' privacy requires controlling access to their data. So, the proposed extended ABAC model suggested in [5] and its components will be used. Again, we specify that we will focus on privacy preserving aspects.

Also, in this scenario we will not focus on the manner on which the privacy group was deducted. The main idea is that privacy preferences are predicted by means of the privacy group defined.

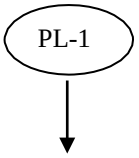
That said, we assume that the patient was able to answer the questionnaire and PPIAMH predict the privacy group to which he belongs.

i. Scenario

Mr. John ELVIS has a cancer tumor. PPIAMH indicates that Mr. John belongs to the fundamentalist group (no trust at all). However, Mr. ELVIS allows his family members and cancer professionals, to view a piece of his sensitive data for better diagnosis; he also allows the sharing of his data with patients having the same assumptions.

ii. Privacy policies generation

PL-1 level corresponding to the Fundamentalist group is used to automatically generate patients preferences sent as rules to the trusted third party to generate the formal privacy policies. Therefore, Mr. John's privacy policies can be defined as follows:



P1: Subjects having the role "Cancer professional" can access my medical data if needed.
P2: Subjects having the organization attribute equal to "Cloud" are not allowed to access my data without my knowledge.
P3: Resource having the category "ordinary" can be viewed by the medical staff working in the hospital.
P4: Subjects having the attribute "social networks" are not authorized to use my medical information.
P5: Subjects having the role "family member" can access to my data if needed.
P6: Subjects having the role "patients with cancer" can collect and use my data.

iii. Access Control Rules

We apply the ABAC model rules defined in the previous section to express the corresponding access control rules. We note that **o.ATTR** specifies object attributes and **s.ATTR** specifies object attributes [5]. We refer to the examples given in [5] to present the access control rules corresponding to the defined privacy policies:

*Rule 1: **P1and P5 policies***

pa_1(s.ATTR, o.ATTR, CTXT, OP):

If **(**(s.ATTR['**role**'] == **Cancer professional** || s.ATTR['**role**'] == **Family member**) && (o.ATTR['type'] == **Medical**) && **purp_assign(**s.ATTR, o.ATTR)=Emergency && OP == {read} **)**

return **allow;**

Rule 2: ***P2 policy***

pa_2(s.ATTR, o.ATTR, CTXT, OP):

if (s.ATTR['**Role**'] == "**Cloud Provider** " && (o.ATTR['**type**'] == **Medical** && **purp_assign(**s.ATTR, o.ATTR)="Advertising" && OP == {read} **)**

return **Deny;**

Rule 3: P6 policy

pa_3(s.ATTR, o.ATTR, CTXT, OP):

if (s.ATTR['**role**']==Patient &&

(o.ATTR['**DiseaseType**'] == Cancer && **purp_assign(**s.ATTR, o.ATTR)="sharing patient's experience" && OP == {read})

return **Allow;**

6. Conclusion

In this paper, we have presented, PPAMH, a privacy-preserving approach for mobile healthcare based on an intelligent mobile application. Our solution aims to help patients to make preferences concerning the disclosure of their sensitive data.

As a future work, we intend first to develop a novel language based on XACML. This language will serve as a tool to standardize patients' privacy policies. Also, we will improve our solution to be applied in mobile platforms. Particularly, we will start by developing the Intelligent Application PPIAMH to allow the distinction of mobile patients in terms of privacy preferences. Also, we will develop a method to generate privacy preferences rules which constitute an important step to generate formal privacy policies.

7. References

[1] Khan, W.Z.; Jazan Univ.; Yang Xiang ; Aalsalem, M.Y. ; Arshad, Q. "Mobile Phone Sensing Systems: A Survey", Communications Surveys & Tutorials, IEEE, 05 February, 2013.pp. 402 - 427

[2] Darrell W. , "How Mobile Devices are Transforming Healthcare", Issues in Technology Innovation, May 2012.

[3] Zhang, J.Y., Pang Wu ; Jiang Zhu ; Hao Hu ; Bonomi, F., "Privacy-Preserved Mobile Sensing through Hybrid Cloud Trust Framework", In proceedings of the Sixth International Conference on Cloud Computing (CLOUD), IEEE , 28 June–3 July 2013, pp 952-953 ,.

[4] S. Sadki, H.El bakkali, "Enhancing privacy on Mobile Health: An integrated privacy module", In Proceedings of the Fifth conference on Next Generation Networks and Services (NGNS), IEEE , 2014, pp. 245 - 250

[5] Subhasish M., W.W. Smari, P. Clemente, J.-F. Lalande, "An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management", Journal of Future Generation Computer Systems, 28-30 May 2014, pp. 147–168

[6] Phoenix strategic perspectives inc (SPI), Survey of Canadians on Privacy-Related Issues", January 2013.

[7] Travis D. Breaux, Ashwini R., "Formal Analysis of Privacy Requirements Specifications for Multi-Tier Applications", 21st International Requirements Engineering Conference (RE), IEEE, 15-19 July 2013, pp. 14 - 23

[8] Ilaria M., Paolo M., Marinella P.,"Prioritized Execution of Privacy Policies", Data Privacy Management and Autonomous Spontaneous Security, Lecture Notes in Computer Science Vol. 7731, 2013, pp 133-145.

[9] A. Westin and Harris Louis Associates, "Harris-equifax consumer privacy survey," Tech. Rep. , conducted for Equifax Inc. 1,255 adults of the U.S. public, 1991

[10] Ponnurangam K., Lorrie Faith C., "Privacy Indexes: A Survey of Westin's Studies", December 2005

[11] Karen Renaud & Dora G´alvez-Cruz, "Privacy: Aspects, Definitions and a Multi-Faceted Privacy Preservation Approach", Information Security for South Africa (ISSA), IEEE, Sandton, Johannesburg, 2-4 Aug. 2010, pp.1-8.

[12] Linke G., Chi Zhang ; Jinyuan S.; Yuguang F., "A Privacy-Preserving Attribute-Based Authentication System for Mobile Health Networks", Transactions on Mobile Computing, Vol. 3 , Issue 9, IEEE, , 16 July 2013, pp 1927 – 1941.

[13] Rongxing L., Xiaodong L. ; Xuemin S., "SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency", Transactions on Parallel and Distributed Systems, Vol. 24 , Issue 3, IEEE, 22 January, 2013 pp 614 - 624.

[14] Sasikanth A.; Amit B.; David K.; "Privacy in Mobile Technology for Personal Healthcare", ACM Computing Surveys (CSUR), Vol. 45 Issue 1, ACM, November 2012.

[15] Sasikanth A.; Amit B.; David K; "A Privacy Framework for Mobile Health and Home-Care Systems", SPIMACS '09 Proceedings of the first ACM workshop on Security and privacy in medical and home-care systems, ACM, November 09 - 13, 2009 pp 1-12.

[16] Anpeng H., Chao C. ; Kaigui B. ; Xiaohui D. ; Min C. ; Hongqiao G. ; Chao M. ; Qian Z. ; Yingrui Z. ; Bingli J. ; Linzhen X., "WE-CARE: An Intelligent Mobile Telecardiology System to Enable mHealth Applications", Journal of Biomedical and Health Informatics, Vol 18, Issue 2, IEEE, 03 March, 2014, pp 693 – 702.

[17] A. Bourouis, M. Feham, M. A Hossain ; "An intelligent mobile based decision support system for retinal disease diagnosis", Journal of Decision Support Systems, Vol. 59, ACM, March 2014, pp 341-350.

[18] Pankaj Deep K., Inderveer Ch., "Cloud based intelligent system for delivering health care as a service", Journal of Computer Methods and Programs in Biomedicine Vol.113, Issue 1, January 2014, pp 346–359.

[19] Earp, J.B., Vail, M. ; Anton, A.I., "Privacy Policy Representation in Web-based Healthcare", In Proceedings of the 40th Annual Hawaii International Conference on System Sciences, IEEE, Hawaii ,January 2007, pp. 138.

[20] Kuang-Wen W., Shaio Yan H., David C. Yen, Irina P., "The effect of online privacy policy on consumer privacy concern and trust", Journal of Computers in Human Behavior Vol. 28, Issue 3, May 2012, pp 889–897.