DOI 10.12694/scpe.v17i3.1181
Scalable Computing: Practice and Experience ISSN 1895-1767
Volume 17, Number 3, pp. 207–226. http://www.scpe.org

RESOLVING CONFLICTING PRIVACY POLICIES IN M-HEALTH BASED ON PRIORITIZATION

SOUAD SADKI* AND HANAN EL BAKKALI†

Abstract. Mobile health has recently gained a lot of attention. Biological, environmental and behavioral data collected from mobile devices can be analyzed and transmitted directly to the person, family or health professionals for immediate and individualized care. However, due to multiplicity of mobile applications and the heterogeneity of actors involved in patient's care, conflicts among the privacy policies defined by the different actors can take place. Thus, we present in this paper an approach to resolve the problem of conflicting privacy policies in e-health/m-health environments using AHP (Analytic Hierarchy Process) prioritization technique. Conflicts detection and resolution are facilitated by the adoption of S4P formal privacy policy language used as a standardized language. Finally, a case study is suggested to illustrate how our solution can be applied to resolve such conflicts.

Key words: Privacy policy; Privacy preference; Conflicting policies; S4P; AHP

AMS subject classifications. 68N30

1. Introduction. The use of technology and electronic communications in healthcare environments, known as e-health, is significantly enhancing patients' quality of care. In fact, Electronic Health Records (EHRs) infrastructures are more enriched in order that the patient become more engaged with his own care, that way he is gradually moving away from a passive to an active role [22]. Particularly, with the emergence of m-health paradigm, as a sub-segment of e-health, and which refers to the use of mobile technologies such as smartphones and tablets, patients are more and more involved in managing their health using mobile applications or personalized services provided by healthcare organizations. More importantly, the lower cost, immediacy and the availability of mobile technologies allows patients accessing their medical history and easily communicate with their doctors whenever and wherever they are. Furthermore, thanks to mobile devices, it becomes so easy for physicians to download medical records, lab results, medical images, and drug information [1]. However, despite the important role mobile technologies play in enhancing patients' quality of care, they also present tremendous drawbacks including privacy violation. Particularly, with the rising number of actors (healthcare organizations, Cloud providers, external services) involved in patients' care, it becomes even harder to protect sensitive medical data but also to know who can or cannot access, collect or share this data across organizations. Hence, in order to ensure data privacy, the sharing, collection and management of medical data must be regulated using privacy policies [3]. These statements or legal documents contain some or all the ways a party manages users' data i.e. what information is collected, how it is collected and under what circumstances this information is used or stored. These privacy policies are expressed using various languages such as natural languages or formal ones like XACML[13], EPAL[14] or P3P[12]. However, the diversity of domains of application, the fixed vocabularies but also the different level of abstraction make these policies highly heterogeneous leading to conflicting situations [3]. Thus, resolving conflicts among privacy policies is of prime importance. Nevertheless, since data collected or shared via computers or mobile devices can be issued from different sources and can be stored in different locations, it is necessary to standardize the privacy policies defined by the different involved parties in order to take the right actions when a conflict occurs. As stated in [5], resolving this kind of conflicts can be very complex and time-consuming especially when the definition of a privacy policy involves more than one party, and the number of possible shared items as well as the entities that can have access to user's data is not fixed or predefined [5]. Some researchers [4-7] believe that the best technique for solving the problem of conflicting privacy policies is by negotiation. Some other works consider prioritization of one policy with respect to the other policy to be the most preferred technique. Still, to the best of our knowledge there is no mature work that properly addresses the issue of conflicting privacy policies in electronic or mobile health environments. We believe that patients' health condition is of prime importance. Because his privacy has a huge impact on his health and outcomes, he has the right to be notified of every action performed on his data. From this

*Mohammed V University,ENSIAS, Information Security Research Team,Rabat MOROCCO (souad.sadki@um5s.net.ma)
†Mohammed V University,ENSIAS, Information Security Research Team,Rabat MOROCCO (h.elbakkali@um5s.net.ma)

perspective, we suggest an approach to solve the aforementioned issue by prioritizing one policy with respect to the other using AHP technique. Our proposed solution adds a different view to the prioritization-based works by allowing an easy criteria extraction from the policy. Furthermore, to facilitate this task, we adopt the S4P language thanks to its flexibility and numerous advantages among which we specify the distinction between services' privacy policies and users privacy preferences. This distinction facilitates conflicts detection since the language syntax allows the satisfaction checking of a third party privacy policy over user's privacy preferences.

The **key contributions** of our work can be summarized as follows:

1. We propose a privacy-preserving approach for solving conflicts among privacy preferences/policies. This approach takes into account the major privacy-by-design principles.
2. We justify the adoption of the S4P languages compared to other languages. Thus, the use of S4P facilitates the translation and conflict detection tasks.
3. We adopt the AHP technique to prioritize the execution of one policy/preference with respect to the other policy/preference.

The rest of the paper is organized as follows: we describe the main problematic through a motivational example in Section 2. Section 3 presents an overview of AHP technique and S4P language followed by our approach description. Section 4 illustrates the efficiency of our solution in solving conflicting policies through a case study. Section 5 presents related work. In Section 6 we conclude the paper and present future work.

2. Problem statement.

2.1. Background. Mobile users are more and more anxious to get into the technology by downloading different computer-based and mobile applications. However, most of these users avoid reading long, complex and time-consuming privacy policies to well understand what of their data has been collected and how it will be used. Instead, they simply click on the 'I agree' without even paying attention to what they are agreeing to. The challenge is to make it as simple as possible for mobile users to define their privacy preference in a comprehensive way that make them avoid reading the complex privacy policies. As for patients, considered as particular users, since they are more and more integrated in the management of their care via computer-based or mobile applications, the communication of their data to different parties may increase their fear over their privacy. Above this, the heterogeneity of these applications as well as the actors involved in patients' care make it even harder to ensure patients' privacy. In particular, most of these actors may possess a privacy policy written in natural language (generally in English), so it should be translated to another language that could be easily understood and interpreted by the other actors. This translation facilitates the detection of any possible conflicts among these policies. In this work, we focus on the issue of conflicting privacy policies in e-health/m-health environments.

2.2. Problem Illustration. In this section, we describe the main problematic through a motivational example of three privacy policies in conflict. The main entities in our example are: The Patient (P), the Hospital (H) allowing patients to track and access their data via Electronic or Personal Health Records (EHR/PHR) and finally the Cloud Povider (CP) that provides storage services for the hospital. Also, the patient can benefit from Cloud-based mobile health apps as shown in Figure 2.1. Also, we assume that each policy is written in a different privacy policy language.

2.2.1. Policies description. Hospital's policy

We assume that H possesses a policy written in XACML language. An XACML policy consists of header information, an optional text description of the policy, a target, one or more rules and an optional set of obligation expressions [23]. Then, the XACML policy is defined in Figure 2.2 as follows.

Patient's preference. Patient's preference is expressed using P2U language. A P2U policy is formed of eight elements : *POLICY element* indicating information about the policy. A policy is created by a provider for a user and with one or more purpose(s) of use [24]. The PROVIDER element referring to the issuer of the privacy policy. USER element i.e. for whom the privacy policy is about [24]. PURPOSE element data sharing purpose, with whom it was shared, for how long it can be retained, and the kinds of data that is relevant for that purpose [24]. CONSUMER element The entity to whom the policy was addressed [24]. RETENTION element The time period (days) for which data can be retained [24]. DATA-GROUP element The group of data that can be shared.

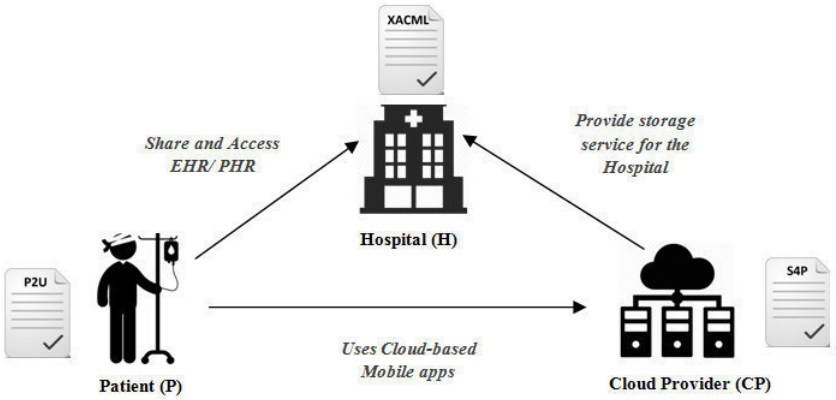


FIG. 2.1. *Ilustrative example architecture*

```
<!-- Permissions specifically for the researcher role -->
<Policy>
<PolicyId="Permissions:specifically:for:the:Researcher:role">
<Rule RuleId="Permission:to:use:medical:data"
Effect="Permit">
<Target>
<Subjects><AnySubject/></Subjects>
<Resources><Medical data/></Resources>
<Actions> <AttributeValue
DataType="&xml;string">Read</AttributeValue></Actions>
<Condition> < purpose="Medical research"/></Condition>
</Target>
</Rule>
</ PolicyId>
</Policy>
```

FIG. 2.2. *Hospital's policy in XACML*

Figure 2.3 presents Patient's privacy preference written in P2U.

Cloud Provider's privacy policy. Using S4P, we assume that Cloud Provider's privacy policy contains the following statement: *CP says CP will save your data for at least 1 year.*

2.2.2. Conflict description. In the first policy, the hospital authorizes any user with the role "Researcher" to use patients' health data for medical purposes whereas patient's policy permits only Health Workers to use/share patient's data (Electronic health record as shown in the attribute DATA) for only medical purposes. Hence the two policies are in conflict since, according to the patient P, researchers are not allowed to use patients' data even for medical reasons. As stated in CP's privacy policy, data can be retained for at least one year while patient's policy indicates that the time of data retention shouldn't exceed 90 days.

The conflict brings out the following concerns:

1. The need for an easy tool allowing the expression of patients' privacy preferences over any action regarding their data.
2. The need for a common privacy language. On one hand, the use of a common language facilitate the communication between the different entities and allows a better understanding of each involved entity's privacy rules on the other hand. Also, this language has to be simple, flexible and reflects both patient's privacy preferences and third parties' policies.
3. The need of a strategy to prevent and resolve any possible conflict.
4. The need of a reference or guidelines indicating the different requirements that should be taken into

```
<POLICY name= "Restrict_access_to_HealthWorker">
  <PROVIDER provID="er60z"/>
  <USER category ="Patient" userID="12" />
  <PURPOSE name="Medical_purpose_only" puID="102">
      <CONSUMER name="HealthWorker"/>
      <RETENTION period="90d" negotiable="TRUE" />
      <DATA-GROUP groupID="ty567" >
        <DATA ref="#medicalrecord" />
      </DATA-GROUP>
  </PURPOSE>
</POLICY>
```

FIG. 2.3. *Patient's privacy preferences in P2U*

account to favorise the execution of a policy, with respect to another one, in case a conflict takes place.

2.3. Overview of privacy laws and regulations. Privacy protection is a shared responsibility between patients, healthcare service providers and any organizations involved in patients' care. However, in order to protect patients' sensitive data from any possible theft or unauthorized use or disclosure, privacy laws and regulations are needed. In US, the Health Insurance Portability and Accountability Act (HIPAA) were created to improve the efficiency and effectiveness of the health care system, by encouraging the development of a health information system by establishing requirements and standards and for the electronic transmission of certain health information [25]. In the same context, the Personal Health Information Protection Act (Canada, 2004) was created with the objective of making patients more engaged with their care and protecting their privacy and the confidentiality of their personal health (PHI) information while facilitating the effective provision of health care by establishing rules for the collection, use and disclosure of PHI [26]. The Enhancing Privacy Protection Act 2012 of Austria defines thirteen privacy principles to protect Australian's personal information, example of these principles topics; Principle 1 open and transparent management of personal information, Principle 6 use or disclosure of personal information; Principle 9 adoption, use or disclosure of government related identifiers [27]. In the EU, the two main directives: the Data Protection Directive 1995/46/EC and the e-Privacy Directive 2002/58/EC [28] regulate the data protection.

3. Prioritization-based approach to resolve conflicting privacy policies. In this section, we describe our prioritization-based approach extending our previous works [2,10]. This work aims to solve the issue of conflicting privacy policies in e-health and m-health environments. We get inspired by the resolution strategy defined in [16] where the prioritization of one policy over another depends on how much that policy is specific in identifying the subject, the object, and the environment to which it is applicable [16]. In fact, in certain cases, it's preferable to prioritize SP's policy execution with respect to patients' preferences. The question is: when and under what circumstances the execution of third parties policies should be prioritized?

To respond to this question, we adopt the multi-criteria decision making AHP technique. The idea is that the execution of a privacy preference depends on the importance/relevance of the criteria extracted from the policies. For instance, let's consider the two following criteria 'purpose of usage' and 'patient's reputation', if the purpose of usage is equal to 'saving patients' life, then the criterion reputation is of lower priority even if it's an important criterion for patient. Also, sometimes access to patients' data is required by Law and the execution of a third party policy is prioritized even if this policy does not match patient's preference. For these reasons, it's of upmost importance to prioritize the execution of a given privacy policy over a privacy preference when a conflict takes place. Next, to formalize patients' and third parties' privacy preferences we adopt S4P language, a formal privacy language for specifying both users' and services' privacy policies.

3.1. S4P: A formal privacy Language. In this part, we justify the adoption of S4P as privacy language where we present its syntax and its advantages compared to other privacy policy languages suggested in the literature. In fact, the comparative study [10] we performed on a number of privacy policies including XACML,

P3P, EPAL and other languages suggested in the literature based on a number of criteria, shows that S4P responds to all the considered requirements. S4P language is human-readable, highly Expressive and can support parameterized behaviours, hierarchical data types, recursive relations, and arbitrary constraints [3]. More interestingly, it distinguishes between users' privacy preferences and services' privacy policies and allows the satisfaction checking between the two [3]. In addition, S4P authorizes delegation of authority which has a crucial role in healthcare. For this purpose, we adopt S4P as a privacy language to express both patients' and healthcare providers' policies. Moreover, thanks to S4P syntax and its flexibility in term of expressing the policies whatever the domain of application, S4P in our work will be used as a standardized privacy language.

S4P syntax. Policies and preferences in S4P are presented in a form of assertions and queries [3]. An assertion in S4P is defined as: $\langle$E says f_0 if $f_1 f_n$ where $C\rangle$ where E defines a user and the f_i are facts and C is a constraint on variables occurring in the assertion [3].
An example of an S4P assertion is : 'Alice says x may use data if x will revoke data within t where t$\leq$ 5 years'.

An S4P query q is defined as follows: Q:: == E says f? | c? | $\neg$ q | $q_1 \wedge q_2 \cup q_1 \sqcup q_2$ | $\exists$ x (q)[3]

An example of an S4P query is :'Alice says HP may share Personal Health Information with other healthcare providers?' [10]

Table 3.1 explains the difference between assertions and queries in S4P.

TABLE 3.1
Assertions and queries in S4P[4,10]

	User preferences	**Service Policy**
Permissions	*May-assertions*: User gives permissions	*May-queries* : Service asks for permissions
Promises	*Will-queries*: User asks for promises	Will-assertions: Service gives promises

Conflicts in S4P. As stated in the previous section, S4P allows the satisfaction checking between users' privacy preferences and services' privacy policies. Thus, using S4P, verifying if a patient's preference is in conflict with a service policy become easier. In fact, checking that a policy satisfies a preference consists of two steps. 1) Every behavior declared as possible in the policy must be permitted by the preference. 2)Every behavior declared as obligatory in the preference must be promised by the policy. In other words, the May-queries and Will-queries must be satisfied as indicated in the following condition [3]:

$$A_{pl} \cup A_{pr} \vdash q_m \wedge q_w \tag{3.1}$$

where A_{pr}, A_{pl}, q_m and q_w respectively designate a set of assertions in patient's privacy preferences, a set of assertions in service provider privacy policies, patient will-queries and service may queries [3].

3.2. Prioritisation with AHP. The Analytic Hierarchy Process(AHP) [8,9] is a multi-criteria and well-known decision making technique based on the evaluation of a set of criteria and alternatives to reach a specific goal. AHP returns thus the most relevant alternative with respect to the set of the pre-selected criteria [16]. Using pairwise comparisons, the relative importance of one criterion over another can be expressed using the ranking in Table 3.2. Also, 2, 4, 6, 8 values are used to represent compromise between the cited priorities .

As stated in [15], The AHP method is based on three principles: 1) model structure ; 2) comparative judgment of the criteria and/or alternatives and 3) synthesis of the priorities [15]. Figure 2.2 summarizes the different steps of this technique.

As shown in Figure 3.1, the first step consists on defining the important criteria. In general, in a decision making process, the criteria constitutes users' requirements. These criteria are grouped in a n*n Matrix called the criteria comparison matrix (C) where n is the number of criteria. The matrix C is then fulfilled using Table 3.1 and then normalized. Next, after determining the most relevant criteria and since the quality of the output of the AHP is related to the consistency of the pairwise comparison judgments [16], the next step consists on calculating the Consistency Ratio (CR) indicating if the matrix is completely inconsistent or if the comparison

TABLE 3.2
Fundamental Scale for AHP [16]

Intensity	Definition	Explanation
1	Equal	Two elements contribute equally to the objective
3	Moderate	One element is slightly more relevant than another
5	Strong	One element is strongly more relevant over another
7	Very strong	One element is very strongly more relevant over another
9	Extreme	One element is extremely more relevant over another

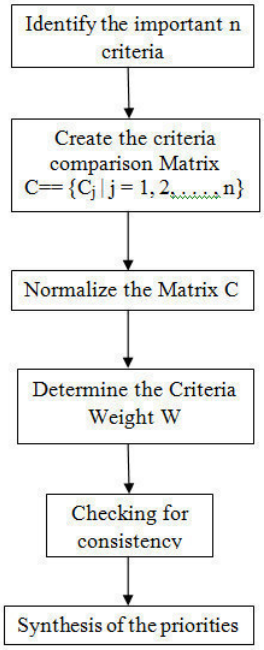


FIG. 3.1. *AHP main steps*

should be recalculated. Finally, the alternatives are evaluated where each alternative is compared with respect to each criteria. The different steps and computing technique are highlighted in the case Study (cf. Sect. 4).

3.3. System architecture and design goals.

3.3.1. System model. In our work, we consider the following entities:

- **Data owner (the patient)**: A patient using health IT (computer-based or mobile applications) to manage his health. In our previous work [2], we classified patients into four main categories as shown in Table 3.3. Thus, a patient can be a Fundamentalist (F), a Pragmatic (P), an Unconcerned (U) or a Should-be-Protected (SPr);
- **Healthcare service providers (Hospital or any entity providing health services)**: in our system a healthcare provider refers to any technology, service or companies offering mobile health apps for their patients;
- **External service providers**: These are entities or companies offering services for healthcare providers including insurance companies, Cloud providers.
- **A trusted third party:** A higher authority complying to privacy laws and standards and playing an intermediary role between patients and SPs. We assume that this party deals with all kind of patients and is responsible for:

-*Translating patients' preferences, HPS's and third parties' policies into Formal policies using S4P*;
-*Suggesting a list of local healthcare providers according to patient's privacy group*;
-*Detecting conflicts among privacy policies.* In fact, since privacy preferences and policies are expressed using a common language, conflict detection is done by applying the rule (1)
-*Extracting the different criteria from S4P policies and preferences in case a conflict occurs.*

TABLE 3.3
Privacy groups [2]

Privacy group	**Description**
Fundamentalist	Patients that distrust third parties to protect their privacy
Pragmatic	Patients who prefer to decide whether they should trust organizations or ask for legal procedures to protect their personal information
Unconcerned	Patients that trust health organizations or any third party to protect their private data.
Should-be-protected	Patients whom health condition does not allow them to make preferences. This group includes children that cant take proper decision and need a guardian or patient badly hurt

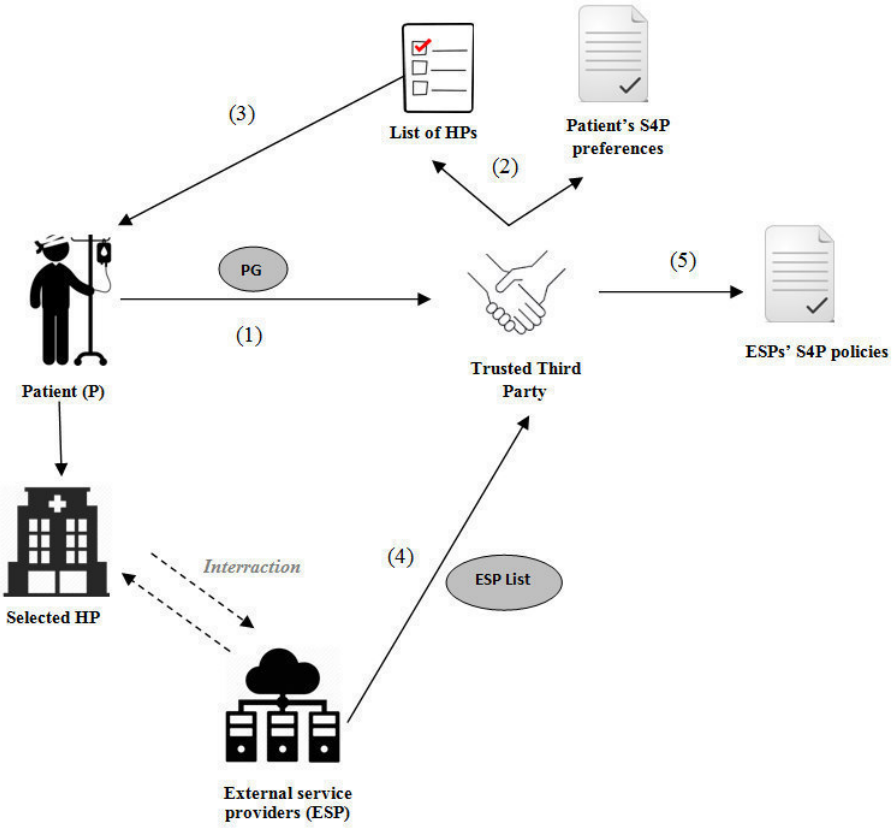


FIG. 3.2. *System architecture and main actors*

The interactions between the four entities are described (see Figure 3.2) as follows:
(1) and (2) : The trusted third party uses patient's privacy group (PG) to formalize his privacy preferences using S4P. As indicated in our previous work (See Figure 3.3) we suggested a Privacy Preserving Approach for Mobile Healthcare (PPAMH) [2] for automatically translating patients' privacy preferences into formal policies.

As shown in the figure, patients are asked to respond to a set of simple questionnaire defined in an intelligent mobile application where the preferences are deduced from patients' answers. The prediction operation is facilitated by grouping the patients into the four groups as stated in the previous section . Then, A set of rules indicating the subjects, the different attributes, constraints, access control decisions that should be taken is then generated and sent to a trusted third party that refers to the generated rules to define the formal privacy preferences. Figure 3.4 presents an overview of the intelligent application. Using the same privacy group and based of the reputation requirement, the TTP selects the local healthcare providers whom privacy policies go along with patient's category. The classification of the HP based on their reputation factor is subject of our future work.

(3) The generated list is then sent to the patient where he selects the HP satisfying his needs (nearest HP for instance). The selected healthcare provider interacts with a number of external entities offering different services.

(4) The list of these external services is then sent to the TTP that seek for their native privacy policies.

(5) In order to check if one of these policies doesn't satisfy patient's privacy preference, ESP's policies expressed in different ways are translated in formal policies using S4P. The idea of having all the policies/ preferences written in the same language facilitates the detection and the prevention of any possible conflict.

It is worth noting that the conflict in our work is provided by other third parties interacting with the healthcare provider 'chosen' by the patient.

3.3.2. Design goals. In order to solve the issue of conflicting privacy policies, we suggest an approach with the privacy-by-design following goals:

- Proactive: That said, in our work we try to prevent the conflict before it happens. In fact, the idea of seeking four healthcare providers responding to patient's need in term of privacy policy reduce the probability of conflict. Also, in case a conflict takes place our solution use this experience to notify the conflicting parties of possible change or improvement in their policy.
- Privacy as the default setting: In the classification of patients we suggested, the should-be-protected-group is considered as a default configuration for patient unable to decide themselves concerning their privacy preferences or patient of the category "Unconcerned".
- Privacy embedded into the design: In every step of the approach we aim to preserve patient's privacy.
- Transparency and visibility: Patient can themselves decide regarding their privacy preferences. As for external services, the fact that they are notified about actions regarding the execution of policies make our solution transparent and visible.
- Respect to user privacy: The integration of the intelligent mobile application allowing a personalized privacy preferences determination and the fact that we select a language distinguishing between patients' policies and users policies make our work patient-centric.

3.4. Application of AHP to determine the prioritized policy/ reference. In this section we answer the question: when and under what circumstances the execution of third parties policies should be prioritized?

The priority of execution in our work is related to:

1. The purpose of usage/disclosure of patients data. Example of purposes: Marketing, research, Law Enforcement, Communication with family, spread of a dangerous disease.
2. Patients' privacy group: In fact, patient's privacy group helps determining the possible important criteria for the patient. For instance for a patient who does not intent to share his information with other parties, we can deduct that the important criteria for this patient are: reputation, time of retention, purpose of usage, collection or divulgation.

In order to resolve a conflict, we consider the following steps:

A. The important criteria identification. Before applying the AHP technique to resolve a possible conflict, it's of up-most importance to determine the different criteria and requirements that should be taken into account. We assume that the definition of these criteria is performed a high authority taking into account the rules and practices defined in privacy laws and regulation. We assume that the considered criteria are: category of data, purpose, reputation, type of organization, time of retention. As stated in the previous section, the classification of patients in four groups in term of privacy preferences plays a crucial role in determining the important criteria defined in Patient's S4P privacy preferences. The structure of S4P policies and preferences

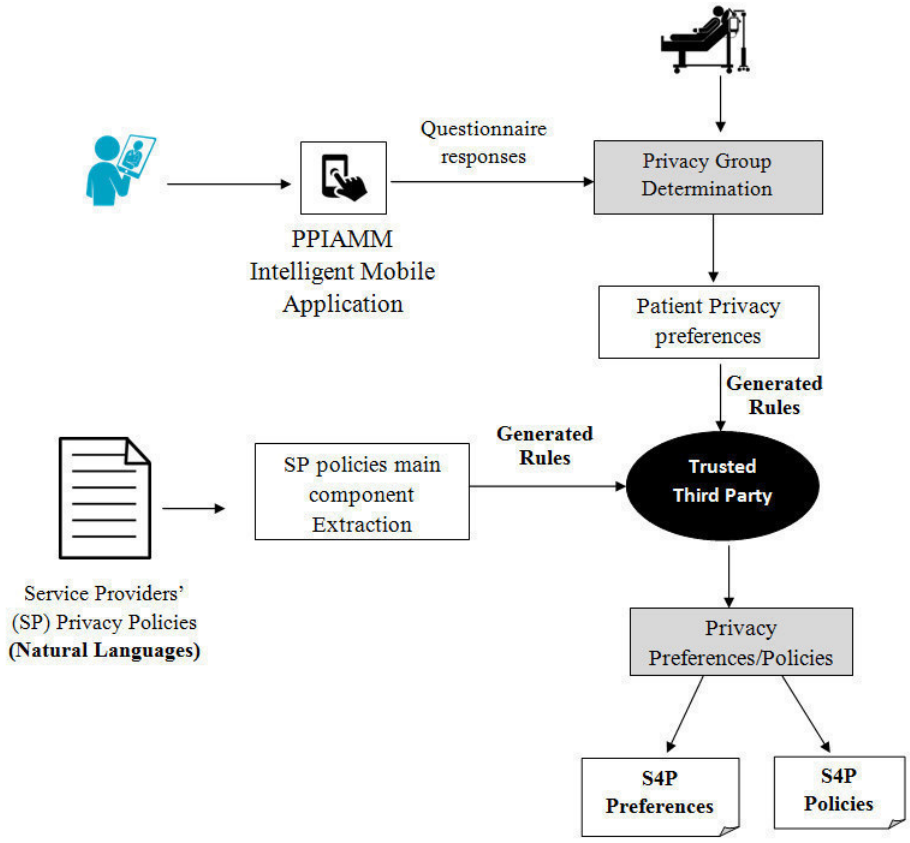


FIG. 3.3. *Privacy prefences policy formalization process [10]*

facilitate the conflict detection as well as the criteria extraction operation as indicated in Table 3.4. We assume that this superior entity is responsible for affecting the initial values (intensity) to the different criteria taking into account patients' condition, rules enforced by law, environment factors etc.

TABLE 3.4
Example of S4P preference/privacy and the associated criteria

Privacy Policy/preference	**Type**	**Extracted criteria**
Alice says **HP** may use Personal Health Information for research purposes?	may-query	Purpose
Alice says **HP** may use Cookies for x if **HP** will revoke Cookies within t where t $\leq$ 1yr	may-assertion	Time of retention
Alice says HP may share Personal Health Information for treatment purposes only [10]	may-assertion	Purpose
Alice says **x** can say **HP** may acess EHR if **x** complies with HIPAA	Delegation of authority	Laws and regulation

B. Creation of the Criteria comparison matrix. A Criteria comparisons Matrix C or a pairwise comparisons matrix is a square matrix which has positive entries and it is reciprocal,i.e., for each element $C_{i,j} = 1/C_{j,i}$ [16].

C. Normalizing the matrix C. Normalizing the matrix means to divide each element in every column by the sum of that column and calculating the average in every column. We obtain the normalized matrix CN.

D. Determination of the most important criteria. We average each row in the normalized matrix CN.

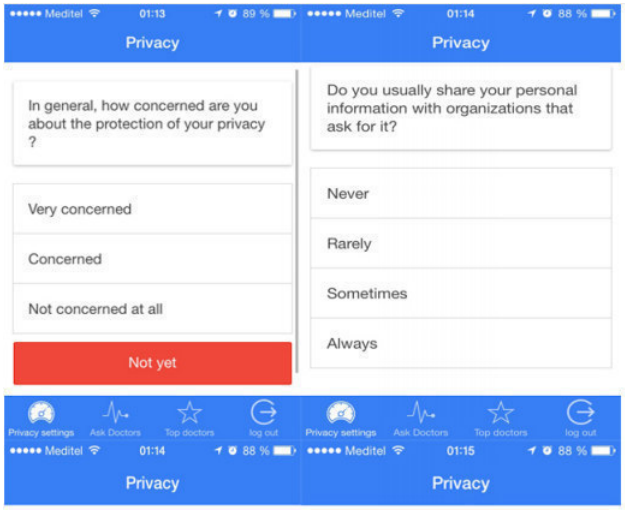


FIG. 3.4. *Example of the PPIMAM intelligent Mobile app*

This average is called "Criteria weight" ,CW. In fact, the highest value of CW constitutes the most important criteria in our design.

E. Checking for consistency. Consistency means that the ranking defined in the Matrix C makes sense. Otherwise, the ranking value should be redefined. In fact, this step requires the computation of a number called CI (consistency index) and then the consistency ratio CR = CI/RI; with a random index called RI, which is a predefined value for each number of criteria. The number 0.1 is the accepted upper limit for CR. If the final consistency ratio exceeds this value, the evaluation procedure has to be repeated to improve consistency. The Algorithm 1 explains the different steps of CR computation and the consistency checking.

Algorithm 1: Consistency checking

input : **C** Comparison Matrix, **n** number of criteria
output: **CS**:Boolean `/* CS= 1 means that C is consistent */`

`/* Calculation of the weight sum vector WS */`
WS = C * CW;
`/* Calculation of the consistency ratio CV */`
CV = WS * (1/CW);
`/* Calculation of the consistency index CI */`
CI = ($\sum CV_{i,j}$-n)/(n-1);
CR = CI/RI;
if $CR < 0{,}1$ **then**
  CS ⟵ 1; `/* The matrice C is consistent */`
end
else
  CS ⟵ 0; `/* The matrice C is inconsistent */`
  Recalculate(C)
end

F. Synthesis of the priorities. Given our two privacy policies, the last step consists on comparing this two alternatives with respect to the n initial criteria. We obtain the matrix AV (alternative value) that will next be multiplied by 1/CW. The final result gives a higher and a lower score. The alternative having the higher value is the policy/preference that should be executed. Thus, as shown in Figure 3.5, we distinguish between

two possible scenarios:

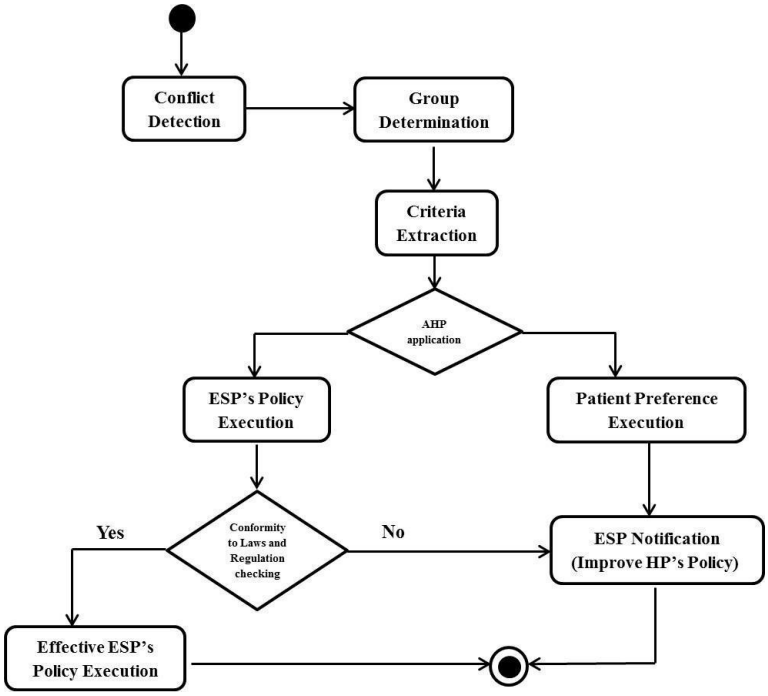


FIG. 3.5. *The approach main steps*

a) The application of AHP indicates that the ESP's privacy policy is executed. In this case TTP verify if this policy is conform to standards and regulations. If it is the case, ESP's policy is executed. Otherwise, TTP notify ESP in question to improve its policy in order to avoid possible future conflicts. It is worth noting that adopting S4P as standard also facilitates the satisfaction checking between ESP's policies and the policies imposed by standards like HIPAA.

b) The application of AHP indicates that Patient's privacy preference is favored. In this case, the ESP is notified of the conflicting situation. In fact, this notification allows third parties to improve their privacy policies statements, especially if the number of conflicts increases continuously.

4. Case Study. In order to illustrate how our approach can be applied to resolve conflicting policies in ehealth/mhealth environments, we consider the conflict scenario suggested in our previous work [10]. As indicated in [10], three main entities are considered:

1) A pediatric medical center in US; Arkansas Childrens Hospital(ACH) [20]; playing the role of a healthcare provider (HP) and which propose a mobile application ,MyACH, to access children's medical history, get information about specific health symptoms and other medical services.

2) CloudTech technologies [21] playing the role of an external service provider that a healthcare provider such as Arkansas can deal with.

3) A 16 years old patient in Arkansas hospital; Bob; whose mother (guardian); Alice; is responsible for any decision or operation regarding his health.

In what follows, our AHP-based approach will be used to resolve the conflict among patient's privacy preferences, healthcare provider's privacy policy and Cloud provider's privacy policy. Since our solution is patient-centric, Bob's privacy preferences (expressed by his guardian) are well defined. Indeed, S4P will be used to formalize bob's privacy preferences and the two providers' privacy policies.

Step 1: Criteria Extraction

The criterion extraction step is preceded by two main steps which are: Privacy/policy formalization and conflict detection.

a) Privacy/policies formalization. Before extracting the different criteria from policies. It is of upmost importance to translate Bob's privacy preferences, ACH hospital's and CloudTech technologies' privacy policies into formal policies using S4P.

Bob's privacy preference: As stated in the previous Section, as the patient group is a key element in our approach, the first step consists on defining this group based on simple questionnaire in a form of intelligent mobile application [2] and that patient is asked to answer. Since Bob is minor, his mother answers these questions in his behalf [10]. We assume that Alice is of the category "Fundamentalist". In other words, she is very strict regarding the sharing, usage and collection of her child. Figure 4.1 presents an example of Bob's privacy preference.

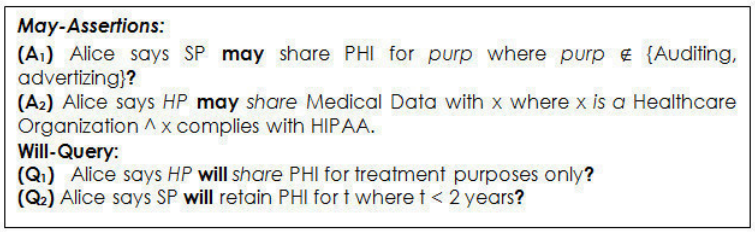


FIG. 4.1. *Bob's privacy preference in S4P [10]*

CloudHealth technologies' privacy policies: CloudHealth technologies' policy are taken verbatim from online CloudHealth technologies' privacy policy. We consider then the following statements:

'We only store data about you for as long as it is reasonably required to fulfill the purposes under which it was first provided by you unless a longer retention period is required or permitted by law' [21].

'We may also use personal information for internal purposes such as auditing, data analysis and research to improve our products' [21].

Table 4.1 shows the translated policies in S4P.

TABLE 4.1
Extract of CloudHealth technologies privacy policy in S4P

English policies	**Translated S4P policies**	**Type**
(A_3)	CloudHealth says CloudHealth will use data for purp where purp ∈ { auditing, data analysis and research }	Will-assertion
(A_4)	CloudHealth says CloudHealth will store personal information for t where t is undetermined	Will-assertion

ACH privacy policy: An extract of ACH Online Privacy policy is taken verbatim [20] and translated into S4P formal privacy polices as shown in Table 4.2.

'We may share some of your PHI with outside people or companies who provide services for us'

'We must disclose your PHI to government authorities that are authorized by law to receive reports of suspected child abuse or neglect involving children or endangered adults'

b) Conflicts detection. As mentioned before, a conflciting situation in S4P means that the may-query in the policy or/and the will-query in the preference are not satisfied where queries are evaluated against the union of the assertions in the policy and the preference [3].

To verify if a conflict takes place, we evaluate each of the three queries Q_1 ,Q_2 ,Q_3 over the union of the will-assertions and may-assertions. i.e. $A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5$. Table 4.3 presents the result of the evaluation of the queries over the assertions. As shown in Table 4.3, the preference (Q_1) is conflicting with the assertions (A_3) and (A_5). In fact, in the preference (Q_1) Alice expresses her desire of sharing her son's medical data for

TABLE 4.2
Extract of ACH privacy policy in S4P

English policies	**Translated S4P policies**	**Type**
(A_5)	ACH says ACH will share your PHI with TP for purp if TP is a government agency where purp $\in$ { child abuse, neglected children, endangered adults}.	Will-assertion
(Q_3)	ACH says ACH may share PHI with outside services?	May-query

medical purposes only. Whereas in the assertions (A_3) and (A_5) ACH and CloudHealth technologies indicates that data can be shared for other purposes. In what follows, we try to find out which of the three conflicting policies is of higher priority using ACH technique.

TABLE 4.3
Evalution of queries against assertions

Query	Satisfied	**Assertions causing conflict**
(Q_1)	No	(A_3) and (A_5)
(Q_2)	No	(A_4)
(Q_3)	No	(A_2)

c) Criteria Extraction. Obviously, the extraction of different criteria from the policies is facilitated thanks to the structure of S4P policies/preferences (facts, constraint, conditions). Concerning the criteria ranking the patient privacy group will help indicating the important criteria for patient even if it is not mentioned in the preference. For instance, for a Fundamentalist patient (Alice's case), we can deduce that the criterion reputation is to be considered as important even if it is not mentioned in patient's preference. Thus, the criterion reputation will be considered during the comparison. Furthermore, other criteria can be extracted from other conflicting situation apart from (Q_1) ,(A_3) and (A_5). For example, we can deduce the criteria 'Time of retention' from the conflict among Alice query (Q_2) and CloudHealth technologies' policy (A_4).

TABLE 4.4
Extracted Criteria from conflicting policies

Preference/policy	**Extracted criteria**
(Q_1)	Purpose , type of data , **reputation**
(A_3)	Purpose
(Q_5)	Purpose, type of data, type of organization, Laws and regulations

Step 2: Application of AHP to resolve the conflict among (Q_1), (A_3), (A_5)

a) The criteria comparison Matrix creation. Using the ranking defined in Table 3.2, we assume that the relevance of each criterion compared to the other criteria is defined as shown in Table 4.5.

b) Determination of the most important criterion. Using BPMSG AHP priority calculator [19],we obtain the priority vector P as indicated in Table 4.6.

As shown in Figure 4.2 presented using online BPMSG AHP priority calculation system [19], the criterion 'Purpose' has the highest value, so the purpose of usage is of higher priority compared to criteria 'Laws and regulation', 'Data category, 'Reputation', 'Type of organization' and 'Time of retention'.

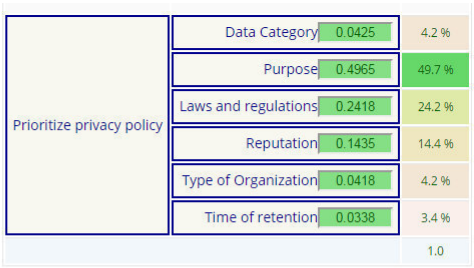
c) Consistency checking. Figure 4.3 indicates that CR=0.048452 $\leqslant 0,1 \Rightarrow$ The matrix is consistent. In other words, the initial value considered for the different criteria were well defined.

TABLE 4.5
Criteria Comparison Matrix C

Criteria	Cat. D	Purp.	Laws and Reg.	Rept.	Tyoe of Org.	TOD.
Category of data	1	1/9	1/7	1/5	1	2
Purpose	9	1	3	5	7	9
Laws and Regulation	7	1/3	1	3	5	7
Reputation	5	1/5	1/3	1	5	5
Type of organization	1	1/7	1/5	1/5	1	1
Time of retention	1/2	1/9	1/7	1/5	1	1

TABLE 4.6
Priority decimal values and priority vector

Criteria	Cat. D	Purp.	Laws and Reg.	Rept.	Tyoe of Org.	TOD.
Category of data	1.0000	0.11111	0.1428	0.2000	1.0000002	2.000
Purpose	9.000	1.000	3.000	5.000	7.000	9.000
Laws and Regulation	7.000	0.3333	1.000	3.000	5.0000	7.000
Reputation	5.000	0.200	0.3333	1.000	5.000	5.000
Type of organization	1.000	0.14285	0.2000	0.200	1.000	1.000
Time of retention	0.5000	0.1111	0.1428	0.200	1.000	1.000
Priority Vector (P)	0.04355	**0.47402**	0.2570	0.1480	0.04277	0.0346



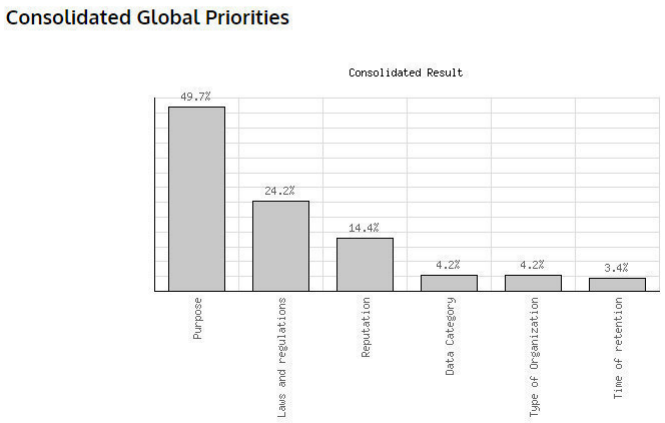


FIG. 4.2. *Criteria Priorities*

FIG. 4.3. *Computation of CR*

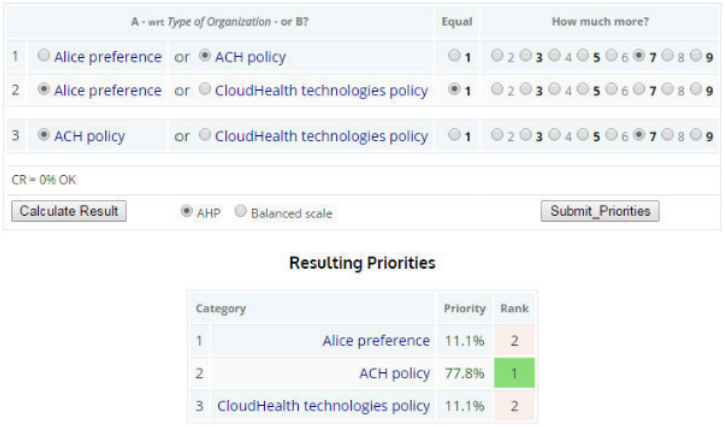


FIG. 4.4. *Comparison of the three policies with respect to the criteria Type of organization*

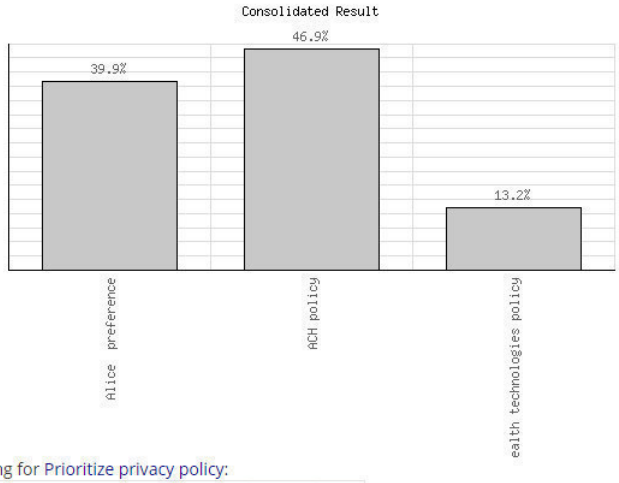
d) Evaluation of the three policies. Now we need to define which of the three policies will be executed. For this purpose we need to evaluate the three alternatives where we compare each of the three S4P policies with respect to the six criteria using AHP technique.

Figure 4.4 presents an example of the comparison of three policies with respect to the criteria "Type of organization" using BPMSG AHP priority calculator system [19]. As shown in Figure 4.4 the criteria type of organization is less important in Alice's preference and CloudHealth technologies' policy than it is in ACH policy.

	Criterion	Node	Glb Priorities	Compare	Alice preference	ACH policy	CloudHealth technologies policy
1.	Data Category	Prioritize privacy policy	4.2%	AHP	0.481	0.405	0.114
2.	Purpose	Prioritize privacy policy	49.7%	AHP	0.458	0.416	0.126
3.	Laws and regulations	Prioritize privacy policy	24.2%	AHP	0.111	0.778	0.111
4.	Reputation	Prioritize privacy policy	14.4%	AHP	0.714	0.143	0.143
5.	Type of Organization	Prioritize privacy policy	4.2%	AHP	0.111	0.778	0.111
6.	Time of retention	Prioritize privacy policy	3.4%	AHP	0.498	0.135	0.367
				Total weight of alternatives:	0.399	0.469	0.132

FIG. 4.5. *Ranking of the three alternatives*

Result for Alternatives



Ranking for Prioritize privacy policy:

	Category	Priority	Rank
1	Alice preference	39.9%	2
2	ACH policy	46.9%	1
3	CloudHealth technologies policy	13.2%	3

FIG. 4.6. *Graphical representation of policies Ranking*

Indeed, if we go back to ACH S4P statements we notice that Government authorities (type of organization) has a strong meaning in the policy. So, we proceed in the same way with the other criteria. Next, using AHP online system, we obtain the result defined in Figure 4.5.

We use the same steps followed in Step 2 to determine the most preferred policy. Finally, as shown in Figure 4.6 ACH policy has a higher priority of 46.9 % compared to Alice preference 39.9 % and CloudHealth Technologies policy 13.2 %.

5. Related Work. In the literature, many privacy-preserving and user-centric works [29, 30, 31, 32, 33, 34, 35, 36, 37] in various domains have been suggested. However, most of these works do not consider the totality of privacy-by-design principles [39]. Also, even if users privacy preferences are taken into account, other

factors such as the multiplicity of actors, the geographic factors or the location of sensitive data can be the cause of privacy violation. For this reason, privacy policies were created regulating the different operations applied to users' sensitive information. As for the medical field, it is important to consider patients as active actors; they have the right to be informed and to take part in any decision regarding the sharing, storage and use of their private and sensitive data. Thus, their privacy preferences need to be properly formalized and taken into account by the different health stakeholders. Nevertheless, these preferences may not be respected by other third parties leading to conflicting situations.

Detecting and solving conflicts among security and privacy policies have recently attracted a lot of attention in different fields. In fact, in order to resolve such conflicts, many approaches and techniques have been adopted. Motivated by the relevance of these works, we developed our approach for healthcare. Indeed, most of the solutions suggested rely on the negotiation technique to resolve such conflicts. Exemplary, authors in [17] suggest a reputation-based approach that makes use of common interest to define other entities having negotiated the same issues in the past, from whom the negotiator can learn the possible offers and counter-offers that could be made to negotiate with the user [17]. In the same context, a negotiation-based approach introducing a policy negotiation point (PNP) between the policy enforcement point (PEP) and the policy decision point (PDP) was suggested in [18] adopting XACML as a privacy language. Other recent negotiation-based works [5-6-7] have been proposed, but noun of them consider the user as an important actor by involving him in the negotiation process. Thus, the challenge is on including the owner of the information (patient in our case) in the decision-making without really forcing him to read complex privacy policies. Furthermore, another work was suggested in [42] describing a policy based authorization infrastructure and a conflict resolution strategy between the different policy decision points. The major particularity of this work is that access to data is always controlled since the users privacy policies are stuck to their data even if this data is shared between Cloud providers or other services [42].

Another category of authors use techniques such as AHP to prioritize the execution of a policy over another. In this context, authors in [16] use a strategy to solve conflicting policies; the prioritization of one policy over another depends on how much that policy is specific in identifying the subject, the object, and the environment to which it is applicable [16]. In the same context, a prototype for solving conflicts in XACML-based e-Health policies was suggested in [6]. Evaluation is done to determine which among the conflicting policies, defines a more specific set of policy elements [6]. In addition to these works, a novel solution for privacy conflict detection and resolution for collaborative data sharing in online social networks was suggested in [43]. The proposed solution considers privacy-sharing tradeoff by quantifying privacy risk and sharing loss [43].

Nevertheless, in order to ensure the effectiveness of these solutions in solving conflicts, they need to be tested before adoption to avoid any possible fault. Indeed, any error in the conception or the usage of a healthcare system may put patients life at risk [44]. From this perspective, a classification of existing testing and verification of healthcare solutions was suggested in [44]. The authors distinguish between three main categories: simulation based methods, formal methods based on mathematics models, and other techniques such as semi-formal methods based on formal syntax and allowing informal semantics [44]. Our work is characterized by adopting a formal language, S4P, to express privacy policies and a formal decision-making methodology, AHP, to resolve the issue of conflicting policies. Still, in order to improve our approach by reducing possible errors in interpreting and translating patients preferences and then extracting the main criteria from these preferences in case a conflict occurs, there is a need for formal validation techniques. For this purpose, model checking can be used. On the other hand, since there are so many actors involved in patients care, most of them with complex architecture, there is a need for formal models that help in verifying and testing the correctness of these systems [45]. In this context, an axiomatic model defining the formal specification requirements for healthcare systems and was suggested in [45]. In particular, with the massive use of Cloud computing services and the emergence of new paradigms such as Big data, healthcare systems are more and more complex. As an example of a Cloud-based work in healthcare, a framework called X1.V1 was suggested in [22] aiming at optimizing the resource utilization on the Cloud by facilitating the exploitation of the cloud elasticity [22]. Thus, using formal methods to enhance the related design issues of Cloud-based systems need to be properly addressed. In this regard, a survey on use of formal methods on testing and verification of Cloud systems was proposed in [50]. Still, and because these systems are considered hybrid where heterogeneous entities collaborate and many

technologies are being used at the same time, there is a lack of a single verification framework for healthcare systems [44].

In addition, it is extremely important to consider the interoperability between the different healthcare actors. For this purpose, health standards like Fast Health Inter-operable Resources (FHIR) [48] have been developed regulating the exchange, integration, sharing and retrieval of electronic medical information and strengthening the reliability of health systems [47]. These standards also need formal methods like model checking to analyze their performance, reliability and functionality [47]. In this regard, a formal probabilistic analysis approach based on the PRISM [46] model checker was proposed in [47] aiming to find the probability of occurrence of wrong results following the FHIR standard. By adopting a formal state-based model for the FHIR, the approach provides more accurate results while allowing additional failures checks and therefore enforcing the reliability of the FHIR standard [47].In the same context, an approach for testing the correctness of device interoperability middleware (DIM) was suggested in [49]. Authors propose to use PRISM model checker to evaluate reliability properties like probability of success and failures and thus take proper measures to design a better DIM. Remarkably, the importance of following health communication standards is also shown in this work where authors use HL7 FHIR standard to illustrate the effectiveness of their proposed solution. Thus, it becomes crucial to follow such standards particularly in distributed environments where data intensive-tasks can be parallelized to improve system performance [51]. Hence, by including FHIR standard into our system design we guarantee an effective and regulated communication between the main actors in our approach especially between the trusted third party and the external service providers. Also, it is of up-most importance to consider compliance to FHIR standard in parallel with privacy conflict checking. That said compliance to FHIR standard need to be classified as crucial criteria in case a conflict take place.

6. Conclusion. In this paper, we presented a technique, applied in e-health/m-health environments, to prioritize the execution of one privacy policy with respect to another when the two policies are in conflict. For this purpose, we adopt the AHP technique and the S4P formal language. This work is an extension of our previous works [2,10] aiming to automatically generate the privacy policies using the notion of *privacy policy group*. The most particularity of our work compared to other AHP-based solutions is the ease of criteria extraction from the policy thanks to S4P syntax structure. Furthermore, the determination of the criteria importance is facilitated by classifying patients into groups in term of privacy preferences. Also, our work respects the major privacy-by-design principles.

As a future work, a comparative study of the most relevant criteria in recent privacy policies mobile health applications will be performed. This study will allow us to develop an automatic mechanism to extract this considered criteria from S4P formal policies. Furthermore, the translation of policies into formal S4P policies will be automated and tested. Finally, the approach will be improved by including an initial step helping patients selecting the most preferred healthcare provider or cloud-based services. For this, the experience of highly reputable parties having offering similar services in the past will be used. The whole system will be evaluated using a formal verification and validation technique.

REFERENCES

[1] B. M Silva, J. Rodrigues, I. De la Torre Díez, M. Lopez-Coronado, *Mobile-Health: A Review of Current State in 2015*, Journal of Biomedical Informatics, June 2015.

[2] S. Sadki, H. El bakkali, *PPAMH: A novel privacy-preserving approach for mobile healthcare*, In Proceedings of the 9th International Conference for Internet Technology and Secured Transactions, IEEE, London December 2014.

[3] L.Y.B. Moritz, M. Alexander, B. Laurent, *AS4P: A Generic Language for Specifying Privacy Preferences and Policies*, Technical report MSR-TR-2010-32, Microsoft Research,2010.

[4] A.A.Datir, A. Sahu,*A Review on Enhancing Privacy Preservation of Web Service through Negotiation Mechanism*,International Journal of Current Engineering and Technology, 2015.

[5] J.M. Such, M. Rovatsos, *Privacy Policy Negotiation in Social Media*,Journal of social and Information Networks December 2014.

[6] A. Lunardelli, I. Matteucci, P. Mori, M. Petrocchi,*A Prototype for Solving Conflicts in XACML-based e-Health Policies*, IEEE 26th International Symposium on Computer-Based Medical Systems (CBMS),2013.

[7] D. Abi Haidar, *Negotiation of sensitive resources using different strategies for policys protection*, Proceedings of the International Conference on Security and management 2013.

[8] T.L. Saaty, *Decision-making with the AHP: Why is the principal eigenvector necessary*. European Journal of Operational Research, 2003
[9] T.L. Saaty, *Decision making with the Analytic Hierarchy Process*. In the International Journal of Services Sciences, 2008.
[10] S. Sadki, H. Bakkali, *A Negotiation-based Approach to Resolve Conflicting Privacy Policies in M-Health*, In International Journal of Information & System Management,2015.
[11] L. Cranor, B. Dobbs, S. Egelman, G. Hogben, J. Humphrey, M. Langheinrich, M. Marchiori, J. Presler-Marshall, M. Reagle, D. Schunter, A. Stampley, R. Wenning *The Platform for Privacy Preferences 1.1 (P3P1.1) Specication*. W3C, 2006
[12] L. Cranor, B. Dobbs, S. Egelman, G. Hogben, J. Humphrey, M. Langheinrich, M. Marchiori, J. Presler-Marshall, M. Reagle, D. Schunter, A. Stampley, R. Wenning *The Platform for Privacy Preferences 1.1 (P3P1.1) Specication*. W3C, 2006
[13] OASIS. *eXtensible Access Control Markup Language (XACML) Version 2.0 Core specification*, 2005
[14] P. Ashley, S. Hada, G. Karjoth, C. Powers, M. Schunter M. *Enterprise Privacy Authorization Language (EPAL 1.2)*. Technical report, IBM, November, 2006
[15] A. Görener, *Comparing AHP and ANP: An Application of Strategic Decisions Making in a Manufacturing Company*, International Journal of Business and Social Science, 2012.
[16] I. Matteucci, P. Mori, M. Petrocchi, *Prioritized execution of privacy policies*, Data Privacy Management and Autonomous Spontaneous Security Volume 7731 of the series Lecture Notes in Computer Science pp 133-145, 2013.
[17] G. Yee, L. Korba, *PThe Negotiation of Privacy Policies in Distance Education*, published in Proceedings. 4th International IRMA Conference. Philadelphia, Pennsylvania, USA, May 18-21, 2003. NRC 44985.
[18] S.Vivying, Y. Cheng, C. Patrick, K. Hung, K. Dickson, W. Chiu, *Enabling Web Services Policy Negotiation with Privacy preserved using XACML*, Proceedings of the 40th Hawaii International Conference on System Sciences - 2007
[19] http://bpmsg.com/academic/ahp_calc.php
[20] Arkansas Children's Hospital. *Joint Notice of Privacy Practices*. http://www.archildrens.org/About-ACH/Privacy-Practices.aspx, revised August 29, 2013.
[21] CloudHeath technologies. *Privacy policy*. http://www.cloudhealthtech.com/privacy. January, 2014
[22] E. Marzini, P. Mori, S. Di Bona, D. Guerri, M. Lettere, L. Ricci, *A Tool for Managing the X1.V1 Platforn on the Cloud*, Scalable Computing: Practice and Experience, Vol. 16, 2015.
[23] OASIS Standard, *eXtensible Access Control Markup Language (XACML) Version 3.0*, 22 January 2013
[24] J. Iyilade, J. Vassileva, *P2U: A Privacy Policy Specification Language for Secondary Data Sharing and Usage*, IEEE Security and Privacy Workshops (SPW), pp. 18-22, 2014
[25] *Health Insurance Portability and Accountability Act of 1996 Public Law 104-191 104th Congress*
[26] *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3, Sched. A
[27] *Australian Privacy Principles and National Privacy Principles Comparison Guide Summary and analysis of key differences for organisations*, April 2013
[28] European Commission, *A comprehensive approach on personal data protection in the European Union*, Brussels, 4.11.2010
[29] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, G. Müller *Aspects of privacy for electronic health records*. International journal of medical informatics 80, e26e31, 2011
[30] J. Li, *Electronic Health Records and the Question of privacy*. Computer, 2013
[31] K. Renaud, D. Gálvez-Cruz, *Privacy: Aspects, Definitions and a Multi-Faceted Privacy Preservation Approach*, Information Security for South Africa (ISSA), 2010
[32] L. Chen, J.-J. Yang, Q. Wang, Y. Niu, *A framework for privacy-preserving healthcare data sharing*, IEEE 14th International Conference on e-Health Networking, Applications and Services (Healthcom), 2012
[33] L. Pang, M-h. S, S-s. Luo, B. Wang, Y. Xin, *Full privacy preserving electronic voting scheme*, The Journal of China Universities of Posts and Telecommunications, 2012
[34] R. Gajanayake, R. Iannella, T. Sahama, *Privacy Oriented Access Control for Electronic Health Records*, Worldwide Web Conference, 2012
[35] D. Jiazhu, L. Shuangyan, L. Hongxia, *A Privacy-preserving Access Control in Outsourced Storage Services*, Computer Science and Automation Engineering , Vol :3, pp 247-251, 2011
[36] B. Lage Srur, V. Muthukumarasany, *Enhancing Trust on e-Government : A decision Fusion Module*, Third International Conference on Network and System Security, 2009
[37] G. Bella, R. Giustolisi, S. Riccobene, *Enforcing privacy in e-commerce by balancing anonymity and trust*. Computers and Security, 30(8), pp 705-718, 2011
[38] Information and Privacy Commissioner of Ontario, Canada *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users*, 2010
[39] M. Assunta Barchiesi, R. Costa, M. Greco, *Enhancing conflict resolution through an AHP-based methodology*, International Journal of Management and Decision Making, volume 13, issue 1, 2014
[40] E. J. Sobczyk, J. Badera, *The problem of developing prospective hard coal deposits from the point of view of social and environmental conflicts with the use of AHP method*, VERZITA, Tom 29, 2013
[41] L. Antonio Bojórquez-Tapia, *A Continual Engagement Approach through Gis-MCDA: Conflict Resolution of Loggerhead Sea Turtle Bycatch in Mexico*, PA51B-2212, December 2015
[42] D.W. Chadwick, K. Fatema, *A privacy preserving authorisation system for the cloud*, Journal of Computer and System Sciences, Vol 78, pp. 13591373, 2012
[43] H. Hongxin , A. Gail-Joon, J. Jorgensen, *Detecting and Resolving Privacy Conflicts for Collaborative Data Sharing in Online Social Networks*, Proceedings of the 27th Annual Computer Security Applications Conference, pp. 103-112 , 2011

[44] A. Gawanmeh, H. Al-Hamadi, M. Al-Qutayri, S. Chin and K. Saleem, *Reliability analysis of healthcare information systems: State of the art and future directions*,Proceedings of the IEEE 17th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 68 - 74, 2015
[45] A. Gawanmeh, *An Axionatic Model for Formal Specifictaion requirements of Ubiquitous Healthcare Systems*, Proceedings of IEEE 10th Consumer Communications and Networking Conference (CCNC), pp. 898 - 902, 2013
[46] M. Kwiatkowska, G. Norman, D. Parker, *PRISM 4.0: Verification of Probabilistic Real-time Systems*, In International Conference on Computer Aided Verification, volume 6806 of LNCS, pp. 585591. Springer, 2011
[47] U. Pervez, O. Hasan, K. Latif, S.Tahar, A. Gawanmeh, M-S Hamdi, *Formal Reliability Analysis of a Typical FHIR Standard based E-Health System using PRISM*, Proceedings of the 1st International Workshop on Reliability of eHealth Information Systems - IEEE HEALTHCOM, pp. 43 - 48, 2014
[48] FHIR. http://www.hl7.org/implement/standards/fhir/
[49] U. Pervez, A. Mahmood, O. Hasan, K. Latif, A. Gawanmeh,*Formal Reliability analysis of Device Interoperability Middleware (DIM) based E-health system using PRISM*, 2015 IEEE 17th International Conference on e-Health Networking, Applications and Services (Healthcom): The 2nd International Workshop on Reliability of eHealth Information Systems (ReHIS), pp. 108 - 113, 2015
[50] A. Gawanmeh, A. Alomari, *Challenges in Formal Methods for Testing and Verification of Cloud Computing Systems*, Scalable Computing: Practice and Experience, Volume 16, Number 3, pp. 321332, 2015
[51] O. Choudhury, N. L. Hazekamp, D. Thain, S.J. Emrich, *Acceleratin Comparative Genomics Workfkows in a Distributed Environmnet with Optimized Data Partictioning and Workflow Fusion*, Scalable Computing: Practice and Experience, Volume 16, Number 1, pp. 5369, 2015

Edited by: Amjad Gawanmeh
Received: Feb 16, 2016
Accepted: Jul 15, 2016