An approach for privacy policies negotiation in mobile health-Cloud environments

Souad SADKI*, Hanan EL BAKKALI
Information Security Research Team - ISeRT
ENSIAS-Mohammed V University
Rabat, Morocco
{souad.sadki, h.elbakkali}@um5s.net.ma

Abstract— **Mobile technologies continue to improve patients' quality of care. Particularly, with the emergence of Cloud-based mobile services and applications, patients can easily communicate with their physicians and receive the care they deserve. However, due to the increased number of privacy threats in mobile and Cloud computing environments, maximizing patients' control over their data becomes a necessity. Thus, formal languages to express their privacy preferences are needed. Besides, because of the diversity of actors involved in patient's care, conflict among privacy policies can take place. In this paper, we present an approach that aims to resolve the problem of conflicting privacy policies based on a Security Policy Negotiation Framework. The major particularity of our solution is that it considers the patient to be a crucial actor in the negotiation process. The different steps of our approach are illustrated through an example of three conflicting privacy policies with different privacy languages.**

Keywords-component; privacy; mobile health, Cloud computing; privacy policy; policy negotiation.

I. INTRODUCTION

Traditionally, the healthcare industry has been one of the slowest fields to adopt new and innovative technologies. Nowadays, with the increased need to continue services and high capacity servers to store patients' medical records at lower cost, more and more healthcare organizations are switching to Cloud computing that presents tremendous benefits. Thanks to this paradigm that has not only changed patient's quality of care but also the way physicians and specialists communicate, medical information can be easily accessed and kept updated so as nurses and doctors can easily find health records and spend more time on providing care to their patients.

The use of mobile technologies in healthcare (m-health) has not only facilitated the exchange and the storage of medical information but in educating patients' on their treatment and medical history as well. Furthermore, the m-Health systems offer innovative abilities, such as, indoor senior residents monitoring, outdoor monitoring and emergency rescue, which may have been very difficult to conduct in the past [21]. Remarkably, the use of smart phones and tablets knows a big growth in Cloud computing as well. Consequently, the concept of mobile health-Cloud has emerged. It refers to the integration of Cloud concept into mobile health environments [21].

However, since different organizations are involved in providing services to patients, one major issue is the difficulty to guarantee confidentiality and privacy on data, especially when data is located in different countries with different laws [22] and different privacy policies (documents that details how users' data is handled [5]). These policies must be made available to customers, and be understandable [23].

Remarkably, since patients become more and more involved in managing their health, they would prefer to define their privacy preferences. Thus, giving them more control over their personal data engenders trust, but this can be difficult in Cloud computing scenarios [23] where many customers are involved. Therefore, the diversity of actors and the heterogeneity of privacy policies defined by these actors lead to conflicting situations that may put patient's privacy at risk. To illustrate this fact, let's consider the example of the conflicting privacy policies defined in [2]. In this example, the patient restricts access to his psychiatric examination to psychiatrics only whereas the policy defined by the healthcare provider allows every practitioner to access all the data of their patients [2]. So, the challenge is on defining formal privacy languages that can easily express patients' preferences as well as third parties privacy policies and then on taking the adequate actions in case a conflict between these policies takes place. To tackle this kind of conflicts, we believe that negotiation is fundamental. In fact, some changes in policies can sometimes save patients' life and improve their outcomes.

In this paper, we present an approach aiming to resolve the problem of conflicting privacy policies in mobile health-Cloud environments through negotiation. Our proposed approach is based on the framework and algorithm defined in [1] to negotiate security policies trying to reach an agreement between two negotiators. The major particularity of our approach is that it does not only consider healthcare and Cloud providers as important participants in the negotiation process but it also looks at the patient as an active actor.

The paper is organized as follows: Section 2 presents a background of conflicting privacy policies in mobile healthcare against Cloud providers followed by related work presentation in Section 3. Section 4 describes our approach illustrated by a case study presented in Section 5. Section 6 summarizes the paper and presents future works.

978-1-4673-8149-9/15/$31.00 ©2015 IEEE

II. PRIVACY POLICIES IN MOBILE HEALTH-CLOUD

Before describing our approach, it's of upmost importance to provide a brief introduction to the notion of privacy in mobile health-Cloud. In fact, privacy is a crucial and challenging issue both in mobile healthcare and Cloud computing environments. On one hand, the utilization of mobile technologies in the health context does not only improve patients' quality of care but also endangers his privacy since almost all mobile health services require access to the internet. On the other hand, the rising consumption of Cloud services by healthcare providers and the emergence of Cloud-based mobile applications multiply privacy threats.

As shown in Figure 1 [7], many actors (Researchers, government, health workers, Mobile Platform Developers …) can gain access to patient's data within an m-health system. Above this, each of these actors can deal with Cloud providers that offer services to multiple organizations. As a result, policies comparison becomes a complex task and the lack of accepted semantics for privacy policies is the main source behind this complexity [24].

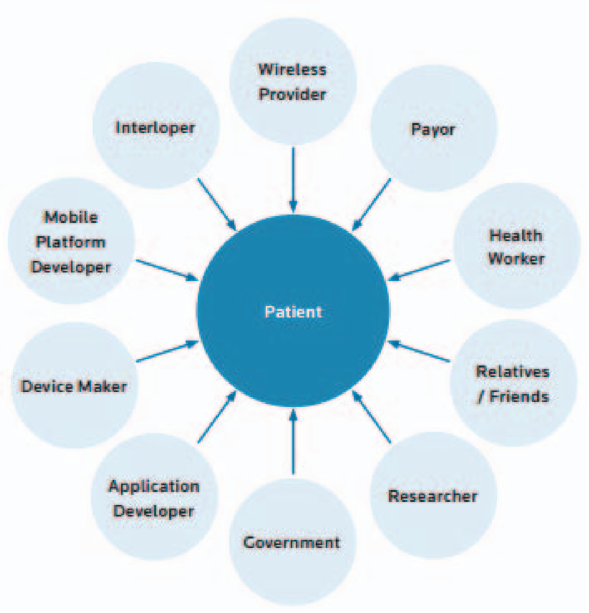


Fig.1. The mHealth Ecosystem Comprises Multiple Actors with Access to Patient Data [7]

In order to preserve customers and providers' privacy, it is important to define privacy policies which describe the way the information is handled, stored and used [25]. These policies should also allow customer (patient in our case) to have a maximum control over the data and processing [25]. However, privacy policies are highly heterogeneous, they are proliferated horizontally (different application domains with varying vocabulary and requirements) and vertically (expressed across all abstraction layers) [5] which lead to conflicting situations. An example of such conflict is given in Section 5.

As a result, efficient mechanisms such as policy negotiation are needed to resolve the issue of conflicting privacy policies and protect patients by taking the right actions at the right time, especially in urgent situations when patient's life becomes the main priority.

III. RELATED WORK

This section presents the state of the art of the some existing privacy policies languages. In particular, we are interested in languages allowing users to express their privacy preferences. Furthermore, we present some recent works that consider negotiation as a fundamental concept to resolve conflicting privacy policies issue. We also focus on recent solutions that consider privacy policies and negotiation in Cloud computing environments.

A. *Privacy policies languages*

There are various privacy policies languages that have been suggested in the literature. Among which we cite EPAL (Enterprise Privacy Authorization Language) [11] and XACML (eXtensible Access Control Markup Language) [10] that is used to define access control policies. However, as stated in [5], XACML do not satisfactorily deal with specifying user preferences and matching them against policies [5].P3P (Privacy Preferences Project) [6] was created to express website's privacy policies in a structured and machine readable way [3]. Nevertheless, policies written in this language can be very complex, and difficult to understand [1]. Also, user preferences cannot be expressed using P3P [5]. Besides, S4P language [5] was created to allow both users' preferences and services provider policies formalization. In the same context, many recent privacy languages consider consumers' privacy preferences. Exemplarily, a privacy language called CPL (Consumer Privacy Language) was suggested in [16]. It reflects user preferences in context-aware services [16]. Also, an efficient policy language tailored to the specifics of Android's middleware semantics was suggested in [15].

B. *Negotiation*

Remarkably, most privacy policies suggested in the literature lack negotiation mechanisms. Some research works have considered negotiation during the development of their solutions. Exemplary, we cite P2U (purpose-to-use) [4], a privacy policy language aiming to enforce privacy and allow a secondary utilization of data on the web [4]. Another example that considers negotiation was proposed in [8], this solution aims to generate a service-level agreement that represents the result of resource negotiation and booking with supported Cloud providers [8]. Also, many negotiation protocols such as FIPA [12] and WS-agreement [13] were developed.

We believe that negotiation should be taken into account when defining privacy languages especially in mobile health-Cloud environments when conflicts occurrence is trivial with the tremendous number of actors included in patients' care.

IV. THE PROPOSED APPROACH

A. *Motivation and design goal*

Our approach aims to resolve conflicting privacy policies in mobile health-Cloud environments. In fact, it extends our previous patient-centric solution entitled Privacy-Preserving Approach for Mobile Healthcare (PPAMH) [17]. Our extended approach is based on the framework defined in [1] aiming at resolving conflicts among XACML security policies.

Also, in order to express patients' privacy preferences, we get inspired by the privacy policy language, Purpose-to-Use (P2U) [4], where the main objective is to preserve privacy and allow users to control the disclosure of their sensitive data [4].

The major particularity of our approach is that it considers the patient as a fundamental negotiator when a conflicting situation occurs. Although users may have very different viewpoints about privacy, it is important to preserve their privacy especially for patients with chronic diseases and those with stigmatized illnesses [14]. From this perspective, our solution aims to protect his privacy preferences and negotiate his privacy policies in his behalf when needed.

In this work, we will not focus on the manner privacy policies are formalized but on what happen when a conflict among heterogeneous privacy policies takes place. More interestingly, since Cloud-based mhealth apps are more and more popular among patients and most healthcare providers are switching to Cloud computing, it becomes necessary to consider this paradigm in recent privacy-preserving solutions.

B. *Overview of PPAMH*

Our previous approach basically aims to facilitate patients' privacy policies formalization by predicting their preferences in a mhealth system. As shown in Figure 2, the first step consists on determining patient privacy group. That said, patient are classified into four main groups [18, 17]

- The *Fundamentalist:* Patients that distrust healthcare organizations or Cloud providers to protect their privacy [17, 18].
- *The Pragmatic*: Patients who prefer to decide whether they should trust organizations or ask for legal procedures to protect their personal information [17,18]
- *The Unconcerned*: Patients that trust health organizations or any third party to protect their private data [17, 18].
- *The Should-Be-Protected*: Patients whom health condition does not allow them to express their privacy preferences. This group includes minors or children that can't take proper decisions and need a guardian or patient badly hurt [17, 18].

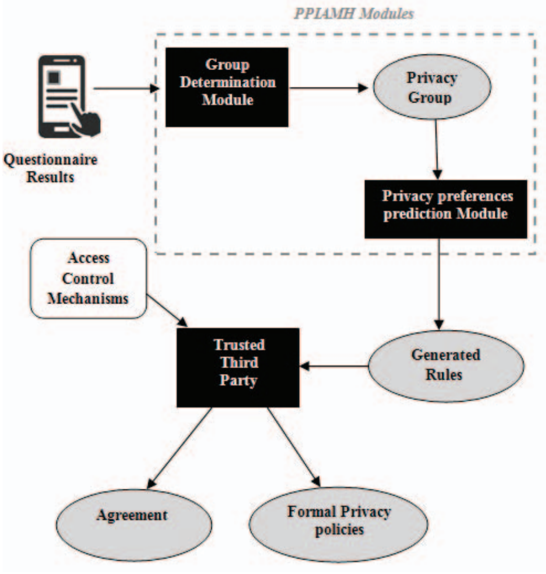


Fig.2. PPAMH main phases [9]

As indicated in Figure 2, patients' privacy preferences are predicted according to the privacy group to which the patient belongs. This predication depends on patients' answers to a simple questionnaire that shows with whom and under what condition a patient would like to share his data. Then, a set of rules is generated and send to a Trusted Third Party allowing privacy preferences expression in a formal way so as they can be interpreted and understood by third parties. After that, an agreement is settled between the trusted third party and third parties forcing them to respect patients' preferences.

We extend this solution by adding a privacy policies negotiation technique where negotiator selection depends on patient's condition, the level of data disclosure he would prefer (privacy groups) as well as the purpose of usage.

C. *Patient privacy policy specification*

To express patient's privacy policies, we refer to P2U (Purpose-To-Use) language that defines eight main elements; (1) POLICY, (2) DATA-PROVIDER, (3) PURPOSE, 4) USER, (5) DATA-CONSUMER, (6) DATA-GROUP and (7) DATA and (8) RETENTION [4.]The main particularity of this language is that it supports negotiation.

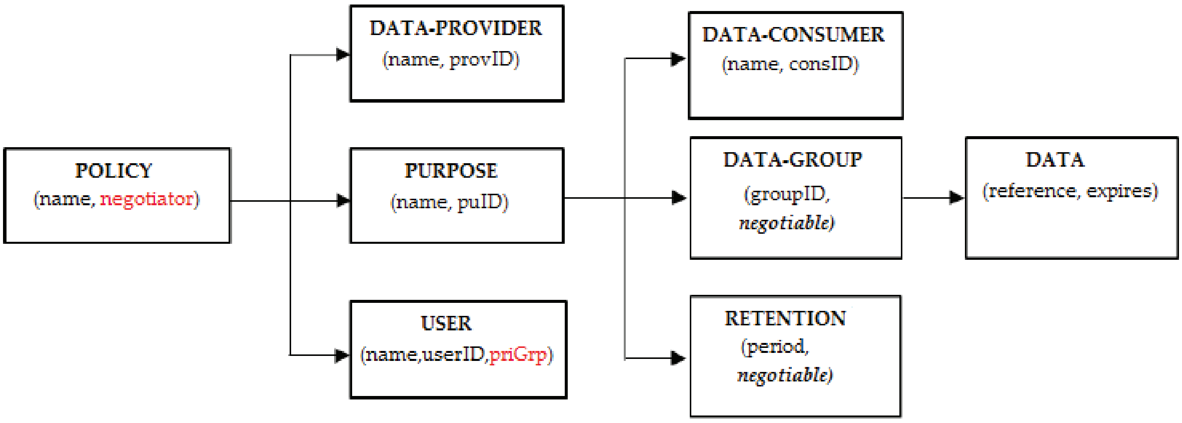


Fig.3. Main elements of P2U Policy Specification Language [4] with the suggested extentions

The eight elements are described as follows:

- **POLICY:** The root element of P2U, the policy is created by a provider for a user and with one or more purpose(s) of use [4]. The purpose of data usage constitutes an important parameter in the negotiation process.
- **PROVIDER:** The issuer of the privacy policy, in our case, we assume that a trusted third party is responsible for formal privacy policy generation.
- **USER**: It specifies user for whom the privacy policy is about [4]. In our case**,** the user is the patient.
- **PURPOSE:** It refers to the 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 [4].
- **CONSUMER:** The entity to whom the policy was addressed [4].
- **RETENTION:** The time period (days) for which data can be retained [4].
- ***DATA-GROUP:*** The group of data that can be shared.
- ***DATA:*** A subgroup of the DATA-GROUP group.

As shown in Figure 3 [4], each element has its attributes. Notably, in this work we will not consider all the attributes of P2U elements. Furthermore, we add some additional attributes such as “priCrp” (privacy group) and “negotiator” to show how negotiation parameter can be injected into the language.

D. Negotiation process description

Our approach is based on the security policy negotiation solution defined in [1] and which was applied to OrBAC policies [19]. According to [1], the negotiation algorithm consists of five actions: propose, receive, create agreement, agreement, refuse and four stages: information stage, demand stage, bargaining stage, contract establishment stage [1].

In this work we will focus on the four stages defined in [1] we add three more additional stages namely: *Conflict detection, Group determination* and *Negotiator determination stages.*

a) Privacy group determination stage

In this phase, the privacy group is determined indicating the category to which the patient belongs. This step has two main objectives: First, it indicates the degree of negotiation required. That said, if the patient for instance belongs to the Fundamentalist group, he will need strong arguments and efforts to agree to negotiation, contrarily to the “Unconcerned” patient who may easily accept negotiating his data. Second, it allows the trusted third party (TTP) to decide whether the patient is able to participate in the negotiation process or not.

b) Conflict detection stage

We assume that TTP recognizes various privacy policies languages. It plays an intermediary role between the patients and other third parties. Therefore, and since privacy policies are heterogeneous, it will be difficult to understand other actors privacy policies. Consequentially, conflict detection becomes a difficult task. TTP plays a vital role as it facilitates the detection of conflicts among different policies.

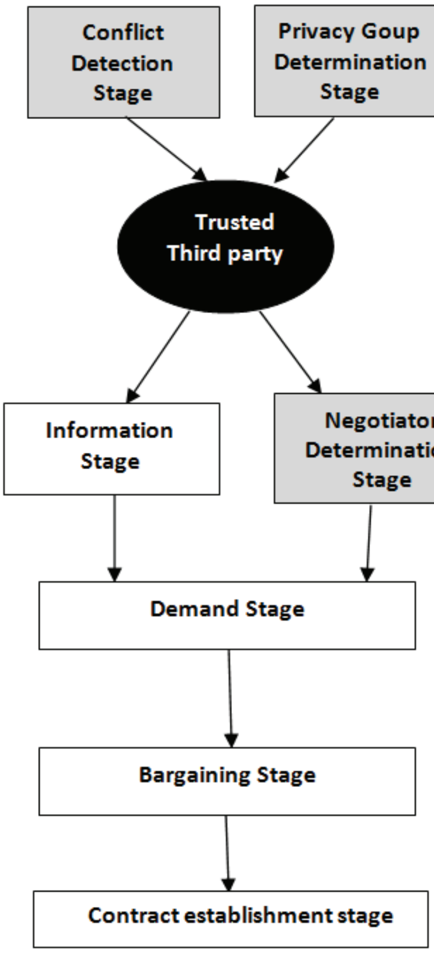

Conflict Detection Stage
Privacy Goup Determination Stage
Trusted Third party
Information Stage
Negotiator Determination Stage
Demand Stage
Bargaining Stage
Contract establishment stage

Fig.4. Main negotiation stages

c) Negotiator determination stage

As stated in [17], we believe that even if a patient can’t make decision to precise his privacy preferences, his privacy must be protected. For this, we define a default privacy policies configuration. So, in this case if a conflict occurs the TTP is responsible for negotiating policies in behalf of the patient.

As shown in Figure 4, the negotiator selection depends on the privacy group to which the patient belongs. If the patient is “Fundamentalist” or “Pragmatic” he can participate in negotiating his policy when a conflict occurs, otherwise TTP becomes the negotiator.

It is worth noting that in urgent situations when patient’s life may be in danger. Saving patient’s life becomes a priority even if some privacy policies would not be respected.

d) Information stage

As mentioned before, the trusted third party can recognize and “understand” numerous privacy policies. Thus, this stage allows patients to understand the involved parties’ policies whatever the language used. Again, TTP plays a primordial role in this stage where it informs other participants of the patient’ privacy group in order to be prepared for the negotiation stage.

e) Demand stage

Each participant sends its offer to its opponent [1]. If the patient (or TTP if the patient is an Unconcerned or a Should-Be-Protected patient) accepts the third party's offer, then a "CreateAgreement" message is sent and the negotiation will enter the contract establishment stage [1]. Otherwise, the two participants enter the bargaining stage.

f) Bargaining stage

The idea is inspired by the bargaining model [1, 20] where two players negotiate how to share one dollar with their changeable attitude from flexible to stubborn [1]. The purpose of this stage is that one of the negotiator or both take a decision [1] (accept or refuse negotiation offer). We note that in this work we will not precise how the bargaining stage is evaluated.

g) Contract establishment stage

In [1], the policy contract is established using OrBAC. In our case we keep the same idea, is that a contract should be settled between the participators indicating the result of the negotiation (Accept, Refuse).

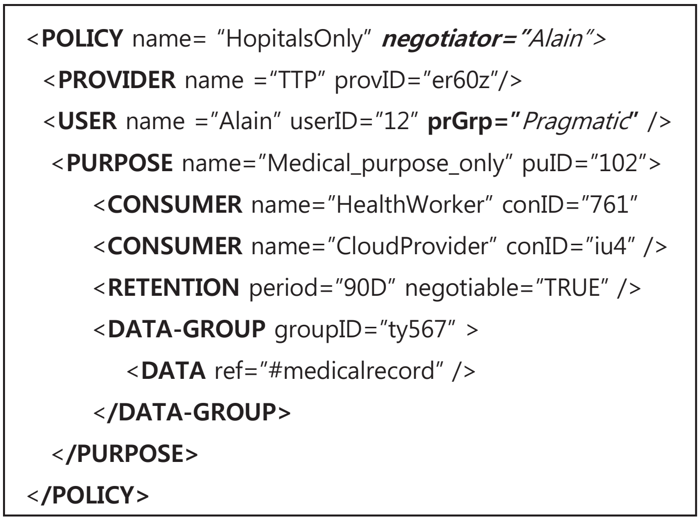
V. A CASE STUDY

A. Policies Formalization

In this section we present an example of conflicting privacy policies formalized in different languages. The purpose is to illustrate how our approach can be used to resolve this conflict.

We consider the three following participants: 1) A patient with the privacy group type "Pragmatic", 2) A Healthcare Provider (HP) and 3) A Cloud Provider (CP). In order to show how TTP can handle the problem of heterogeneous policies and detect the conflict. We assume that P2U is used to express the patient policies whereas S4P is used to formalize the Cloud provider policies and XACML to express HP policy.

Po.1: Patient policy using P2U (simplified XMLformat)



```
<POLICY name= "HopitalsOnly" negotiator="Alain">
  <PROVIDER name ="TTP" provID="er60z"/>
  <USER name ="Alain" userID="12" prGrp="Pragmatic" />
   <PURPOSE name="Medical_purpose_only" puID="102">
        <CONSUMER name="HealthWorker" conID="761"
        <CONSUMER name="CloudProvider" conID="iu4" />
        <RETENTION period="90D" negotiable="TRUE" />
        <DATA-GROUP groupID="ty567" >
            <DATA ref="#medicalrecord" />
        </DATA-GROUP>
   </PURPOSE>
</POLICY>
```

In **Po.1** policy, the patient Alain who belongs to the *Pragmatic* category allows the hospital worker with the ID 761 to use his health record for medical purpose only. Since Alain is a "Pragmatic" patient, he can negotiate his privacy policy if a conflict occurs.

Po.2: HP policy using XACML language

Subject having the role "Researcher" and with the ID "761" can use patients data for statistical purpose.

Po.3: CP policy using S4P language

CP says CP will save medical data for at least 1 year.

- Po.1 and Po.2 policies are conflicting. In effect, the patient Alain (Pragmatic) allows the Health Worker (who is at the same time a professor researcher) having the ID 761 to access his medical information for medical usage only. In contrast, the healthcare provider allows the researcher with ID 761 to access patient data for statistical (non medical purpose)

- Po.2 and Po.3 policies are conflicting. Alain allows the CP to retain his data for a period less than 90 days where CP policy indicates that data can be saved for at least 1 year.

B. Application of the approach

In this section we show how our approach can be used to resolve the conflict among Po.1 and Po.3

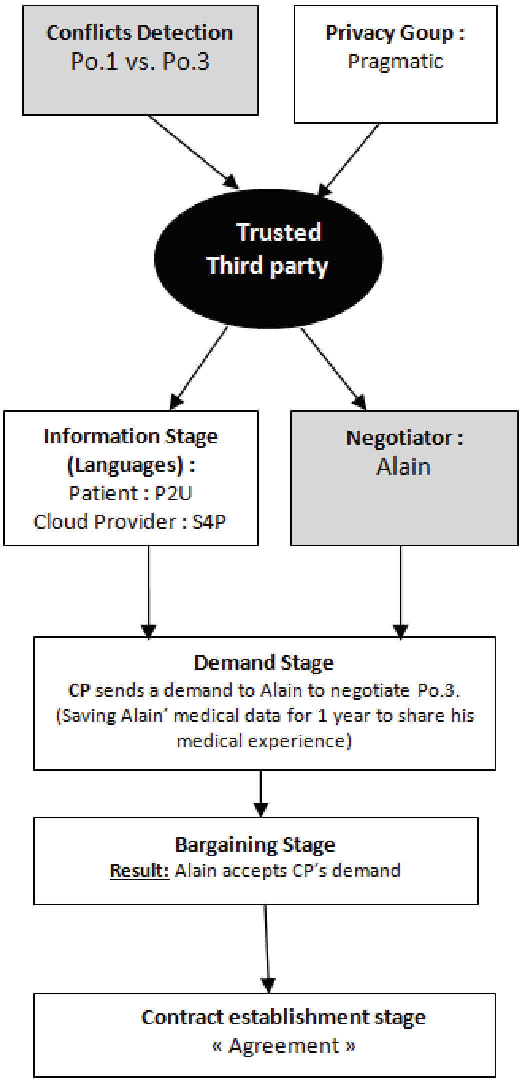


Fig.5. Application of the negotiation approach to resolve the conflict among Po.1 and Po.3

Figure 5 presents the main steps to resolve the conflict between Po.1 and Po.3. After specifying the privacy group to which Alain belongs (Pragmatic), his privacy preferences are predicted using our previous method [17]. After Alain' privacy policies formalization using P2U language is performed, the TTP deducts the 'consumers" of data (third parties), determines their languages (XACMP and S4P) and seek for possible conflicts.

TTP detects a conflict among Po.1 and Po.3 and check if the patient can be involved in the negotiation process (otherwise TTP is responsible for negotiation). Therefore, since Alain is an active actor he received the Cloud demand to save his data longer for statistical purpose. In This case Alain accepts to negotiate his privacy (Bargaining stage) because his is convinced of the purpose of usage and accepts the CP demand.

Finally, an agreement is settled between Alain and CP indicating the success of the negotiation (Contract establishment stage).

VI. Conclusion

In this paper, we have presented a patient-centric approach to resolve conflicting privacy policies in mobile health-Cloud. Our approach is based on a security policy negotiation framework. We tried through this paper to treat different issues including the heterogeneity of privacy policies as well as the multiplicity of actors including Cloud Computing providers.

Our work is characterized by classifying patients into groups in terms of privacy preferences which makes resolving conflicts among policies easier. Then, to show the utilization of the extended approach, we have considered a real-world example of conflicting policies which shows how our extended solution can be used to resolve the conflict with three different privacy languages: P2U, XACML and S4P.

As a future work, we intend to develop each stage of the approach, in particular the bargaining stage which constitutes a crucial step towards resolving conflicting privacy/ preferences policies in mobile health-Cloud.

References

[1] Y. Li, N. Cuppens-Boulahia, J-M. Crom, F. Cuppens and V. Frey, "Reaching Agreement in Security Policy Negotiation", IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 98 – 105, 2014.

[2] A. Lunardelli, I. Matteucci, P. Mori, M. Petrocchi., " A prototype for solving conflicts in XACML-based e-Health policies", IEEE 25th International Symposium on Computer-Based Medical Systems (CBMS), pp. 449 – 452, 2013.

[3] M. Y. Becker, A. Malkis, L. Bussard; "A practical generic privacy language", ACM Proceedings of the 6th International Conference on Information Systems Security, pp. 124-139, 2010.

[4] 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 .

[5] M. Y. Becker, A. Malkis, L. Bussard, "S4P: A Generic Language for Specifying Privacy Preferences and Policies", Technical report MSR-TR-2010-32, Microsoft Research, 2010.

[6] L. Cranor, B. Dobbs, S. Egelman, G. Hogben, J. Humphrey, M. Langheinrich, M. Marchiori, M. Presler-Marshall, J. Reagle, M. Schunter, D. A. Stampley, and R. Wenning. "The Platform for Privacy Preferences 1.1" (P3P1.1) Specication. W3C, Nov. 2006.

[7] TrustLaw, Mhealthalliance, Ker & MCKenzi, MSDbewell, "Patient privacy in a mobile world: A framework to address privacy law in mobile health", June 2013.

[8] S. Venticinque, R. Aversa, B. Di Martino, M. Rak and D. Petcu, "A Cloud Agency for SLA Negotiation and Management", Springer Parallel Processing Workshops, Lecture Notes in Computer Science Volume 6586, pp 587-594, 2011.

[9] S.Sadki and H El Bakkali, "A Patient-Centric Approach for Intelligent Privacy Policies Generation in Mobile Healthcare", International Journal of e-Healthcare Information Systems (IJe-HIS), Vol.1, Issue 1/2/3/4,pp. 2-9,2014.

[10] OASIS. eXtensible Access Control Markup Language (XACML) Version 2.0 core speci_cation, 2005.

[11] P. Ashley, S. Hada, G. Karjoth, C. Powers, and M. Schunter. Enterprise Privacy Authorization Language (EPAL 1.2). Technical report, IBM, Nov 2003.

[12] FIPA Specification, "Foundation for intelligent physical agents," Geneva, Switzerland, 2002.

[13] O. Waldrich et al., "Ws-agreement negotiation version 1.0," in Recomendation,Open Grid Forum (May 2011), 2011.

[14] J. Li, "Privacy policies for health social networking ",Journal of the American Medical Informatics Association: JAMIA, April 2013.

[15] S. Bugiel, S. Heuser, "Flexible and Fine-Grained Mandatory Access Control on Android for Diverse Security and Privacy Policies", Proceedings of the 22nd USENIX Security Symposium., 2013.

[16] G. M. Kapitsaki, " Reflecting User Privacy Preferences in Context-Aware Web Services", IEEE 20th International Conference on Web Services (ICWS), pp. 123 – 130, 2013.

[17] S, Sadki; H. El BAKKALI, "PPAMH: A novel privacy-preserving approach for mobile healthcare",9th International Conference on Internet Technology and Secured Transactions pp. 209 – 214, 2014.

[18] A. Westin and Harris Louis Associates, "Harris-equifax consumer privacy survey" Tech. Rep. , conducted for Equifax Inc. 1,245 adults of the U.S. public, 1991.

[19] A. A. E. Kalam, R. Baida, P. Balbiani, S. Benferhat, F. Cuppens,Y. Deswarte, A. Miege, C. Saurel, and G. Trouessin, "Organization based access control," , Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks, pp. 120–131, 2003.

[20] E. Burato and M. Cristani, "The process of reaching agreement in meaning negotiation," in Transactions on Computational Collective Intelligence VII Springer , pp. 1-22, 2012.

[21] B. Xu, L. Xu; H. Cai ; L. Jiang,"Architecture of M-Health Monitoring System based on Cloud Computing for Elderly Homes Application ",IEEE Enterprise Systems Conference ,pp. 45-50,2014

[22] S. Das, Sudip Misra, M. Khatua and J. J. P. C. Rodrigues, "Mapping of sensor nodes with servers in a mobile Health-Cloud environment", IEEE 15th International Conference on e-Health Networking, Applications & Services (Healthcom), pp. 481 – 485, 2013.

[23] S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services",Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, pp 44-52,2009

[24] N. Papanikolaoua, S. Creeseb and M. Goldsmithb,"Refinement Checking for Privacy Policies, journal of Science of Computer Programming," Vol. 77, Issues 10–11, pp. 1198–1209, 2012.

[25] H. Mouratidisa, S. Islama, C. Kalloniatisb and S. Gritzalisc."A framework to support selection of cloud providers based on security andprivacy requirements",Journal of Journal of Systems and Software, Vol. 86, Issue 9, pp. 2276–2293, 2013.