A Semantic Model for Personal Consent Management

Ozgu Can

Ege University, Department of Computer Engineering,
35100 Bornova-Izmir, Turkey
ozgu.can@ege.edu.tr

Abstract. Data protection and privacy has a significant importance in information sharing mechanisms, especially in domains that handle with sensitive information. The knowledge that can be inferred from this sensitive information may unveil the consumer's personal information. Consumers should control who can access their consent data and for what purposes this data will be used. Therefore, information sharing requires effective policies to protect the personal data and to ensure the consumer's privacy needs. As different consumers have different privacy levels, each consumer should determine one's own consent policy. Besides ensuring personal privacy, information sharing to obtain personal data usage for acceptable reasons should be endorsed. This work proposes a semantic web based personal consent management model. In this model, consumers specify their consent data and create their personal consent policy for their consent data according to their privacy concerns. Thus, personalized consumer privacy for consent management will be ensured and reasonable information sharing for the personal data usage will be supported.

Keywords: Consent Management, Privacy, Semantic Web.

1 Introduction

The remarkable growth in digitization of records brings great advances for consumers. However, sharing personal information brings significant privacy risks for consumers, like *linking attack*. Linking attack is the leakage of a crucial private information by integrating released and publicly available data sets. Therefore, an adversary can track the individuals identity. According to the study of 1990 U.S. Census summary data in [1], 87% of the individuals in the United States are identifiable with their gender, date of birth and 5-digit zip code of their addresses. [2] presents problems and risks of data mining to patient privacy by cross linking the patient data with other publicly available databases, processes such as data mining may associate an individual with specific diagnoses. Thus, consumers must control the access to their personal records and give consent to others who want to access these records. Consent management is a policy that allows a consumer to determine rights for a provider's access control request to one's personal information. On the other hand, the balance between

E. Garoufallou and J. Greenberg (Eds.): MTSR 2013, CCIS 390, pp. 146–151, 2013.

the personal privacy and the quality of service should be ensured. The goal in consent management is stimulating information sharing to improve the quality of the personal data usage for specific acceptable reasons and protecting personal privacy according to personal consent policy. Medical domain is one of the inevitable field to realize the importance of consent management. Patients, who are the subjects of electronic health records (EHRs), have the right to know who is collecting, storing or processing their data and for what purpose this is being done [3]. Health information systems (HIS) must protect patient's consent rights. As each patient may demand different privacy levels for their EHRs, it will not be efficient to use a standard privacy policy for EHRs. Therefore, in this work, a practical personal consent management model is proposed and illustrated for the healthcare domain. In the example model, each patient can specify one's own consent data according to one's personal privacy needs and create personal consent policy. Each access request to one's EHRs are executed according to one's personal consent policy. As a result, the decision of this access request should be a permission or a prohibition.

The goal of the paper is to describe a semantic web based personal consent management model to protect consumer privacy while endorsing reasonable information sharing for personal data usage. In order to achieve this goal, patient information and HIS are chosen as the object and the domain of the sample consent policy, respectively. The paper is organized as follows: Section 2 informs the relevant related work. Section 3 explains the consent management model. Section 4 presents a case study example of the proposed model. Finally, Section 5 expresses the direction of the future work.

2 Related Work

The protection of consumer's user information, especially in health systems, is one of the crucial need for systems to provide consumer's privacy. Recent works can be categorized in two forms that one is for the generalization of published records and the other is controlling access to records. The former work is based on record anonymization to protect user data before publishing it [4] [5] [6]. The latter work is based on access control techniques. [7] proposes a design principle of an electronic consent system and develops a health transaction model. In [8]; threats to the confidentiality, integrity and availability of personal health information are discussed and a security policy model for clinical information systems is given. The approach in [9] uses the domain model, the policy model, the role model, the privilege management model, the authorization model, the access control model and the information distance model for authorization and access control of electronic health record systems. Consentir, a system for patients information and their consent policies are presented in [10]. Consentir supports five different consent policies for patient consent management. Clinical Management of Behavioral Health Services (CMBHS, `http://www.dshs.state.tx.us/cmbhs`) is a web-based, open source electronic health record. Users of the system are assigned to roles that determines their access level. The system allows patients or

their legally authorized representative's (LAR) to determine what data can be seen and by whom. Patients or their LAR can also revoke or modify the terms of their consent. The consent form is then integrated with the patient's record in the Electronic Health Record (EHR) system. In Virtual Lifetime Electronic Record (VLER) Health Community project, patients can control access to their personal health information, including medication lists, lab test results and diagnoses. HIPAAT (`http://www.hipaat.com`) develops consent management and auditing software for personal health information (PHI) privacy. A trust management system, named as Cassandra, uses electronic health record system as a case study [11]. It is a role based trust management system for access control in a distributed system. The study in [12] focuses on creating and managing of patient consent with the integration of the Composite Privacy Consent Directive Domain Analysis Model of the HL7 and the IHE Basic Patient Privacy Consents (BPPC) profile. [13] describes a framework for enforcing consent policies for healthcare systems based on workflows. Permissions are assigned to subjects who want to access patient's consent. The context of the framework is expressed in terms of workflows.

The proposed consent management model differs from the relevant works in that we combine access control techniques with personalization based on semantic web technologies. In our work, the user manages the access to one's records and controls the privacy of one's data. In order to give the user full control of one's own data, user data is differentiated in two directions: quasi-identifiers and medical data. The main goal in differentiating the user data is to eliminate the risk of linking attack.

3 Consent Management Model

The consent management model consists of the following sets: Subject, User, Role, Organization, Action, Object, Quasi-Identifier, Constraint, Purpose, Policy Objects and Consent Data Policy.

- A *subject* is the owner of data that is going to be accessed.
- *User* is an entity that wants to access to the subject's data and perform actions on this data.
- Each user and subject has a *role* and a set of attributes. For example, users of the health care system can be in a nurse role or a doctor role or a lab technician role.
- An *organization* is an entity where a user is an employee of.
- An *action* indicates operations that a user can perform on an object. For example, updating, viewing or deleting a record. In consent management model, actions are also used by subjects to define operations that they permit or prohibit on their EHRs.
- An *object* is an entity that a user wants to access and perform actions on. An object represents subject's consent data. For example, in a HIS example, objects are medical records of patients' personal health information.

- A *quasi-identifier* is an entity that is determined by a subject to define a privacy requirement value on. Quasi-identifier is a set of attributes in a table which can be linked with external information to re-identify the individuals identity [14]. This set consists of attributes that identify subjects from others uniquely e.g.,age, gender, social security number, zip code and so on.
- A *constraint* is a condition that is used to limit the definitions of an entity related to policy objects.
- *Purpose* states user's intentions on an object.
- *Policy objects* define what actions can a user perform on an object and under what circumstances. Policy object can be a permission or a prohibition. Permission means what an entity can do and prohibition means what an entity can't do.
- *Consent data policy* is the subject's policy definition to finalize the access decision.

The access request has a tuple of $\langle User, Subject, Object, Action, Purpose\rangle$. Consent data policy, which is the respond of the request, is represented as a tuple of $\langle Subject, User, PolicyObject, ConsentData\rangle$. Consent data set is a pair of $\langle Subject, Quasi-Identifiers\rangle$ or $\langle Subject, Object\rangle$. Policy object is formed of $\langle Role, Action, Purpose, Constraint\rangle$. The model is represented with a DL $\mathcal{ALCQ}$ language and has the following atomic concepts and roles:

- atomic concepts are Subject, User, Role, Organization, Action, Object, Quasi-Identifier, Purpose, Policy Objects, Consent Data and Consent DataPolicy.
- the atomic role hasRole links a user and a subject to a role.
- the atomic role isAnEmployee links a users to an organization.
- the atomic roles isOwnerOf and hasOwner are inverse roles and create a link between a subject and an object.
- the atomic role hasRequest links a user to a subject and subject's consent data.
- the atomic role hasConsentPolicy links a subject's consent to a user's request.
- the atomic role hasConsent links subject and consent data to policy objects.
- the atomic role hasConstraint links actions and policy objects to constraints.
- the atomic role hasQuasiIdentifier links a subject to a quasi-identifier.
- the atomic role hasAction links a policy object to an action.

The consent management model rules have the following forms:

$\forall Subject\ hasRole(Subject, Role),\ \ Role \sqsubseteq hasRole.Subject$
$\forall User\ hasRole(User, Role),\ \ Role \sqsubseteq hasRole.User$
$\exists User\ isAnEmployee(User, Organization)$
$Organization \sqsubseteq isAnEmployee.User$
$\forall Object(hasOwner(Object, Subject)) \leftrightarrow \exists Subject(isOwnerOf(Subject, Object))$
$\exists Subject(hasQI(Subject, QuasiIdentifier))$
$\exists Subject(hasConsentData(Subject, ConsentData))$
$\forall PolicyObjects(hasAction(PolicyObjects, Action))$
$CD \equiv S \sqcap (\exists hasQuasiIdentifier.Subject \sqcup \exists isOwnerOf.Subject)$
$U \times S \times O \times A \times P \rightarrow hasRequest.User$
$S \times U \times PO \times CD \rightarrow hasConsentPolicy.Subject$
$R \times A \times P \times T \times \rightarrow PO$
$Permission \equiv \neg Prohibition$ and $Prohibition \equiv \neg Permission$

4 A Case Study

In this section, we illustrate a practical example of the consent management model for electronic health information systems. The example model is illustrated according to the syntax given in the previous section. In the case study, Bob is the doctor of Mary, who has quasi-identifiers and the owner of the `BloodTest` result file:

$hasRole(Bob) \equiv Doctor$
$isAnEmployee(Bob, MedicalCityHospital)$
$isDoctorOf(Bob, Mary) \equiv hasPatient(Bob, Mary)$
$hasRole(Mary) \equiv Patient$
$hasDoctor(Mary, Bob) \equiv isPatientOf(Mary, Bob)$
$isOwnerOf(Mary, BloodTest)$
$hasQuasiIdentifier(Mary, (Name, Gender, DateOfBirth, SocialSecurityNumber))$

Bob makes two requests to publish his patient Mary's quasi-identifiers and `BloodTest` result for his `Research` purpose:

$hasRequest1(Bob) = (Bob, Mary, Publish, QuasiIdentifier, Research)$
$hasRequest2(Bob) = (Bob, Mary, Publish, BloodTest, Research)$

Mary defines two consent data concept that includes her quasi-identifiers and `BloodTest` result, respectively:

$CD1(Mary) = hasConsentData(Mary, QuasiIdentifier)$
$CD2(Mary) = hasConsentData(Mary, BloodTest)$

Mary defines permission for the request to her `BloodTest` result from doctors who are her responsible doctors in order to publish her result for `Research` purpose:

$PermissionDoctor = (Doctor, Publish, Research, DoctorOfPatient(Mary))$

On the other hand, Mary prohibits Bob to publish her quasi-identifiers for his `Research` purpose:

$ProhibitionQI = (Doctor, Publish, Research, DoctorOfPatient(Mary))$

The final responses to Bob's requests will be Mary's consent policies respective to requests:

$hasConsentPolicy1(Mary) = (Mary, Bob, ProhibitionQI, CD1(Mary))$
$hasConsentPolicy2(Mary) = (Mary, Bob, PermissionDoctor, CD2(Mary))$

The first consent policy includes the consent data concept named `CD1(Mary)`. Similarly, the second consent policy includes `CD2(Mary)`. In this manner, Mary can control who can access to her personal records and for what purposes these data can be used. She can categorize her records as consent data and determine access levels according to the request's purpose. Eventually, she allows the usage of her personal data while protecting her privacy.

5 Conclusion

In the proposed consent management model, users can manage who can access which part of their data under what circumstances and for what purposes. Thus, users not only protect their privacy, but also contribute to improve the quality of the personal data usage for specific acceptable reasons. As a future work, the consent policy ontologies of the proposed model will be created and queried to execute and test scenarios of the model. Roles of the consent management model will be represented with Friend-Of-A Friend (FOAF, `http://www.foaf-project.org`) profiles. A reasoning engine will also be developed to demonstrate the use of consent policy rules.

References

1. Sweeney, L.: Uniqueness of Simple Demographics in the U.S. Population. Technical Report, Carnegie Mellon University (2000)
2. Cooper, T., Collman, J.: Managing Information Security and Privacy in Healthcare Data Mining: State of the Art. Medical Informatics: Knowledge Management and Data Mining in Biomedicine 8, 95–137 (2005)
3. Kluge, E.-H.W.: Informed consent and the security of the electronic health record (EHR): Some policy considerations. International Journal of Medical Informatics 73(3), 229–234 (2004)
4. Sweeney, L.: k-Anonymity: A Model for Protecting Privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems 10(5), 557–570 (2002)
5. Machanavajjhala, A., Gehrke, J., Kifer, D., Venkitasubramaniam, M.: ℓ-Diversity: Privacy Beyond k-Anonymity. In: Proceedings of the 22nd International Conference on Data Engineering (ICDE 2006), p. 24 (2006)
6. Li, N., Li, T., Venkatasubramanian, S.: t-Closeness: Privacy Beyond k-Anonymity and ℓ-Diversity. In: Proc. of Int. Conf. on Data Engineering (ICDE 2007) (2007)
7. Coiera, E., Clarke, R.: e-Consent: The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment. Journal of the American Medical Informatics Association 11(2), 129–140 (2004)
8. Anderson, R.J.: A Security Policy Model for Clinical Information Systems. In: Proceedings of the 1996 IEEE Symposium on Security and Privacy (1996)
9. Blobel, B.: Authorisation and Access Control for Electronic Health Record Systems. International Journal of Medical Informatics 73(3), 251–257 (2004)
10. Khan, A., Nadi, S.: Consentir: An Electronic Patient Consent Management System. In: 4th Annual Symposium of Health Technology (2010)
11. Becker, M.Y., Sewell, P.: Cassandra: Flexible Trust Management, Applied to Electronic Health Records. In: Proceedings of the 17th IEEE Computer Security Foundations Workshop (CSFW 2004), pp. 139–154 (2004)
12. Ko, Y.-Y., Liou, D.-M.: The Study of Managing the Personal Consent in the Electronic Healthcare Environment. World Academy of Science, Engineering and Technology 65, 314 (2010)
13. Russello, G., Dong, C., Dulay, N.: Consent-based Workflows for Healthcare Management. In: Proceedings of the 2008 IEEE Workshop on Policies for Distributed Systems and Networks (2008)
14. Samarati, P.: Protecting Respondents Identities in Microdata Release. IEEE Transactions on Knowledge and Data Engineering 13(6), 1010–1027 (2001)