ENHANCING PATIENT INFORMATION SHARING THROUGH SOCIAL NETWORKS

M. Poulymenopoulou, D. Papakonstantinou, F. Malamateniou and G. Vassilacopoulos
Department of Digital Systems, University of Piraeus, Karaoli & Dimitriou 80, Piraeus, Greece

Keywords: Social network, Personal health records, Access control services.

Abstract: Currently, there is an effort for empowering patient self-care and improving the traditional healthcare delivery models by expanding the concept of healthcare though the provision of advanced online healthcare services. Those services require increased level of information flow and collaboration among patients and healthcare professionals. This collaboration and patient information sharing can be achieved by integrating social networks functionality with personal health records, based on open standards. In fact, social networking exists to facilitate communication and collaboration and make possible what was only recently impractical in healthcare, such as trans-regional clinician collaboration through web-based broadcasting systems, therefore integrating the information included into personal health records. Along these lines, this paper presents a secure middleware that aims at enabling patient information sharing among patients and healthcare professionals through social networks functionality and applications, giving particular emphasis to a security architecture that enforces access control services for protecting the disclosure of patient private information to unauthorized users.

1 INTRODUCTION

In healthcare the traditional "face-to-face" healthcare delivery may not fully meet the new requirements of "e-Patients", who wish to sit at home seeking healthcare consultancy or online help instead of lining up hours just for a few minutes talk with physicians in hospitals or clinics (Domingo, 2010); (Greene et al., 2011). However, the reality is that few online healthcare services can be found. Recently, the Health 2.0 movement aims at promoting participatory healthcare by suggesting the collaboration among patients, caregivers, medical professionals and other healthcare stakeholders through the use of Web 2.0 technologies like social networks (SNs) (Domingo, 2010); (Gajanayake et al., 2011); (Thompson et al., 2011).

The social-networking revolution is coming to healthcare, at the same time that new Internet technologies and software programs are making it easier than ever for healthcare professionals to find timely, personalized health information online and for patients to self-manage their medical information and share it with others (Domingo, 2010); (Gajanayake et al., 2011). Moreover, several healthcare social networks (HSNs) have emerged, such as PatientsLikeMe, Inspire.com, MedHelp, Sermo and Ozmosis. HSNs provide online technical infrastructures for physicians to share clinical cases, images, videos and medical knowledge and for patients to promote disease awareness, and positive and proactive behavior, in order to stay healthy while living with a disease (Domingo, 2010); (Greene et al., 2011).

Since communication is a critical weakness of the healthcare delivery system, SNs could potentially improve communication by establishing permanent channels (network connections) among multiple physicians and between physicians and patients. Also SNs can make the health system more available, responsive and personalized to the public by providing access to eHealth services to both the public and health professionals (Domingo, 2010); (Thompson et al., 2011); (Williams, 2010). Most of the eHealth services (e.g. diagnosis, self-treatment, expert advice, second medical opinion) require the availability of accurate and updated patient medical information and therefore some HSNs support quantified self-tracking by providing easy-to-use data entry screens for condition, symptom, treatment and other biological information.

Poulymenopoulou M., Papakonstantinou D., Malamateniou F. and Vassilacopoulos G..
ENHANCING PATIENT INFORMATION SHARING THROUGH SOCIAL NETWORKS.
DOI: 10.5220/0003772203780381
In *Proceedings of the International Conference on Health Informatics* (HEALTHINF-2012), pages 378-381
ISBN: 978-989-8425-88-1
Copyright © 2012 SCITEPRESS (Science and Technology Publications, Lda.)

At the same time, there is an increasing interest by patients on public web-based Personal Health Records (PHRs) for coordinating their lifelong health information and make appropriate parts of it available to those who need it (Cushman et al., 2010); (Shachak et al., 2010); (Sunyaev et al., 2010). However, PHRs are mostly designed to meet the needs of episodic clinical encounters between patients and health care professionals, and around the diagnosis and treatment of diseases (Greene et al., 2011); (Shachak et al, 2010).

Sharing patient data existing on PHRs through SNs can provide the required patient information to healthcare professionals, administrators and other using eHealth services. However, the issues of patient information security and privacy are some of the biggest concerns when exposing patient private information to a social network. Many SNs allow users to customize some privacy settings and some online HSNs provide an opportunity to freely obtain and disclose information about a health condition without having to divulge one's identity. In addition, most web-based PHRs like Microsoft Health Vault and ICW LifeSensor, provide functionality for filtering the medical data to be shared with others (Gajanayake et al., 2011); (Sunyaev et al., 2010). However, there are still open issues as concerns PHRs and SNs privacy and security and therefore patients and practitioners still worry about the wrongful dissemination of medical information. Nevertheless, currently there are no available guidelines to help navigate these complex issues (Cushman et al., 2010); (Thompson et al., 2011); (Williams, 2010).

The focus of this paper is on the security aspects of the middleware without compromising the benefits of information sharing, thus increasing the overall social value of SNs in healthcare. Hence, a context-aware access control service is proposed that extends PHR access control features and enables sharing of patient data through SNs.

2 MOTIVATION

The basic motivation of this research stems from our involvement in a recent project concerned with the employment of a middleware-level solution to enable patient medical information sharing from PHRs to advanced eHealth services (online diagnosis, expert advice, disease management) that are provided through SNs using their functionality. Among the requirements of this middleware was to enable patients setting their access control sharing preferences on their medical information existing on PHRs. The security requirements of this middleware motivated this work and provide the context for the development of access control services for the middleware based on a security architecture that ensures authorized patient information sharing from PHRs in the domain of SNs, according to specific user context-based preferences.

To this end, according to the overall middleware architecture a) advanced eHealth services are provided using SN functionality (e.g. messaging mechanisms), b) integrated patient information (patients active medical problems, diagnosis, treatment plans and latest medical tests results) exists on PHR and controlled by patients, c) the middleware provides functionality for retrieving patient information from PHR, transforming this into a standard format and sending it to requesting SN users and d) the access control services of the middleware enable setting and enforcing the users access control policies for their medical information.

3 SECURITY ARCHITECTURE

According to the proposed cloud-based middleware architecture, as presented in Figure 1, an application server and an XML base are configured at cloud servers. At the application server exist the middleware services that encapsulate middleware functionality, the web and cloud services used by the access control services, the context-based access control mechanism that takes context-based authorization decisions for accessing (read access is only allowed through the SN) patient medical data existing on PHRs and the context manager that hosts the ontology created to represent context information. At the XML base are stored the user access control policies. This architecture takes the stance that the medical data of PHRs is retrieved in the form of XML documents according to clinical standards, as the Continuation of Care Document (CCD) or the Continuation of Care Record (CCR).

As far as concerns the ontology, Ontology Web Language (OWL) files have been created that enable context information sharing in a semantic way and also context reasoning. Additionally, Semantic Web Rule Language (SWRL) rules have been written to capture additional relationships among domain classes (Beimel et al., 2011).

Context information involves a) user social information, such as user profiles, relationships, groups and activities on the SN (e.g. online/offline, chatting), b) medical data information that includes

data elements of PHRs as proposed by CCD/CCR XML schemas and involves problems, medications, alerts, procedures, results and other and c) temporal information, such as time instances or time intervals.

In Figure 2 a small part of the ontology created in OWL is shown. Context information of the domain ontology is used to set contextual constraints on user medical data (stored on PHRs) sharing preferences. Hence, contextual constraints are divided to a) user social based constraints that are specified at user level, at user group level, at SN relationship level (that links users), at user current activity level (e.g. user participation on group online chat), b) medical data based constraints that are specified at the medical data element level and c) temporal based constraints (e.g. time interval) (Wrona et al., 2005).

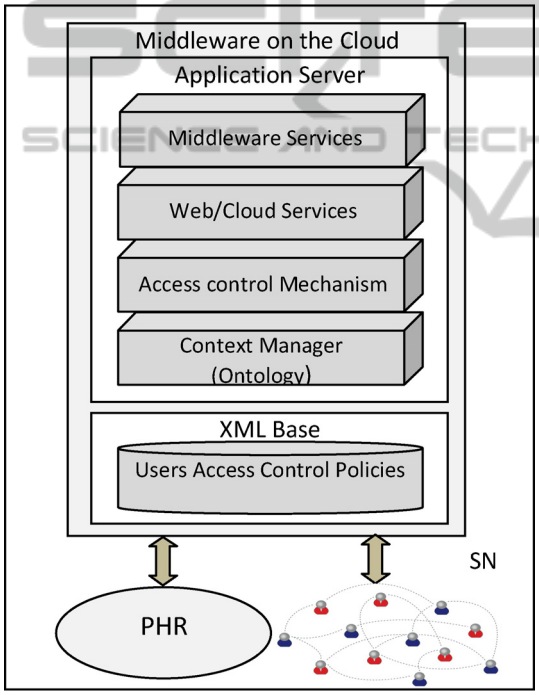

Figure 1: The middleware architecture.

According to the security architecture, users set through web service calls their context-aware sharing preferences. Then, the access control mechanism communicates with the context manager to consult the ontology and the relevant SWRL rules in order to result in new context information and thus, (if any) new contextual constraints. The user sharing preferences according to contextual constraints (initial and inferred) are translated to context-based access control rules and are stored by cloud services to the cloud servers in the form of user access control policy. Thus, for example, a user access control rule can specify that his/her current medications can be shared only with users that are members of his groups named 'mydoctors' and 'mypharmacists'. Another user access control rule may specify that patient psychological profile can be read during an online psychotherapy group without disclosing patient identity, only by the authenticated users of that group and only for the time period the online group therapy takes place.

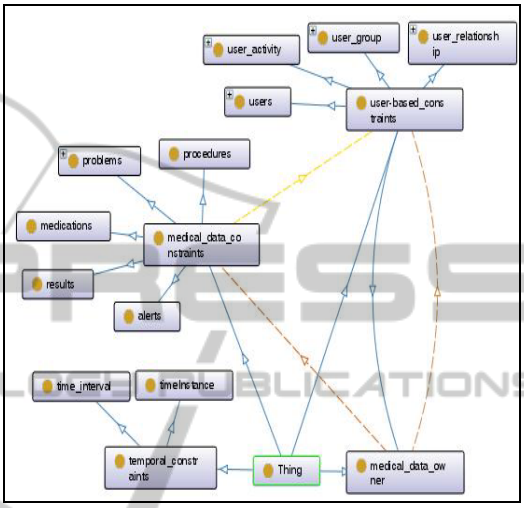

Figure 2: A small part of the OWL ontology.

On SN user request for accessing another (target) SN user medical data, web services are called to communicate with the context-aware access control mechanism to retrieve the (target) user access control policy, to evaluate the appropriate access control rules and take decisions for the patient data elements that should be viewed. Then, middleware services are called that encapsulate functionality for retrieving allowed patient data XML elements from patient PHR, structuring this data in the form of a CCD-based document and sending it to authorized requesting user using SN messaging mechanisms. For example, a physician might request through SN (e.g. SN application) to view a patient latest laboratory test results. Then, the appropriate web services are called to evaluate patient access control rules and if access is allowed the test results are structured in the form of a CDD document that is sent to the requesting user by SN message or email.

4 PROTOTYPE IMPLEMENTATION

To illustrate the feasibility of the proposed security

architecture, a prototype implementation is presented that is under development. Without the loss of generality, for the purpose of the prototype experimental implementation are used the public cloud infrastructure of Amazon, the social network of Facebook and the PHR of Microsoft called HealthVault. Web services based on REST technology were developed using the open source Jersey to implement the access control services of the middleware as well as the middleware functionality. The HealthVault Application SDK was used to access data from Microsoft HealthVault PHR. Regarding the access control mechanism implementation, the XML access control language (XACML) is used and XACML policies are created to represent user sharing preferences that are stored to the cloud servers using Amazon S3 service (Wrona et al., 2005). In addition, a web application loaded in the context of Facebook is created to provide the user application interface to access the access control services and the middleware functionality.

5 CONCLUDING REMARKS

This paper presents a security architecture that aims at promoting secure patient information sharing among users at anytime and from anywhere through the use of SNs that are always available by any device. In particular, the proposed access control services ensure authorized patient information retrieval from PHRs and its provision through SNs messaging mechanisms and applications/tools according to user's access control preferences. To realize this, there is a need to balance the urge to protect individuals from potential harm that may be caused by exposing personal information through SNs and therefore to ensure that high quality healthcare can be provided through the use of eHealth services. In this paper, only the issue of what other users can see has been addressed. Questions of how to prevent the organisation in control of the SN site using personal data which has been freely shared for commercial gain through SN functionality are left unanswered. Finally, there are other problems not addressed here, such as legal and ethical issues (Cushman et al., 2010).

The proposed security approach constitutes a technological solution that is clearly implementable. At present the development of the prototype is still in the early stage. Thus, testing, user acceptance, validation, evaluation and performance count on real use of the eHealth services are still to be done.

REFERENCES

Beimel, D. and Peleg, M., 2011. 'Using OWL and SWRL to represent and reason with situation-based access control policies', *Data and Knowledge Engineering*, vol. 70, pp. 596-615.

Cushman, R., Froomkin, M., Cava, A., Abril, P. and Goodman, K., 2010. 'Ethical, legal and social issues for personal health records and applications', *Journal of Biomedical Informatics*, vol. 43, pp. S51-S55.

Domingo, M., 2010. 'Managing healthcare through social network', *IEEE Computer Society*, vol. 43, no. 7, pp. 20-25.

Gajanayake, R., Iannella, R. and Sahama, T., 2011. 'Sharing with care: An information accountability perspective', *IEEE Computer Society,* vol. 15, no. 4, pp 31-38.

Greene, J., Choudhry, N., Kilabuk, E. and Shrank, W., 2011. 'Online social networking by patients with diabetes: A qualitative evaluation of communication with Facebook', *Journal of General Internal Medicine*, vol. 26, no. 3, pp. 287-292.

Shachak, A. and Jadad, A., 2010. 'Electronic health records in the age of social networks and global telecommunications', *Journal of the American Medical Association*, vol. 303, no. 5, pp. 452-453.

Sunyaev, A., Kaletsch, A. and Krcmar, H., 2010. 'Comparative evaluation of Google health api vs. Microsoft Helathvault api', *International Conference on Health Informatics - HEALTHINF 2010*, Valencia, Spain, pp. 195-201.

Thompson, L., Black, E., Duff, P., Black, N., Saliba, H. and Dawson, K., 2011. 'Protected health information on social networking sites: Ethical and legal considerations', *Journal of Medical Internet Research*, vol. 13, no. 1.

Williams, J., 2010. 'Social networking applications in health care: threats to the privacy and security of health information', *Proceedings of the 2010 ICSE Workshop on Software Engineering in Health Care*, Cape Town, South Africa, pp. 39-49.

Wrona, K. and Gomez, L., 2005. 'Context-aware security and secure context-awareness in ubiquitous computing environments', *Proceedings of the XII Autumn Meeting of Polish Information Processing Society Conference*, pp. 255-265.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS