

Towards a Privacy Access Control Model for e-Healthcare Services

Patrick C. K. Hung

Faculty of Business and Information Technology
University of Ontario Institute of Technology (UOIT), Canada
Patrick.Hung@uoit.ca

Abstract

Information privacy is usually concerned with the confidentiality of personal identifiable information (PII) and protected health information (PHI) such as electronic medical records. Thus, the information access control mechanism for e-Healthcare services must be embedded with privacy-enhancing technologies. Role-based Access Control (RBAC) model has been widely investigating and applying into various applications. This paper proposes a framework of RBAC with privacy-based extensions to tackle such a need in e-Healthcare services.

Keywords: Role-based Access Control (RBAC), Privacy, e-Healthcare Services, Web Services.

1. Introduction and Motivation

In today's era of e-Healthcare informatics, there is a constant and growing need for automated and integrated views of health information to guide rapidly changing health planning activities and increasingly sophisticated health-related policymaking, as well as fulfilling the information requirements of daily e-clinical care and e-patient management [1]. Privacy is one of the major issues to be handled in such an environment. Access control is the process of limiting access to the resources of a system only to authorized users, programs, processes, or other systems. Access control is synonymous with controlled access and limited access. In general, access control is defined as the mechanism by which users are permitted access to resources according to their identities authentication and associated privileges authorization [3]. Role-based Access Control (RBAC) model has been widely investigating and applying into various applications for a period of time [4]. Permissions are associated with roles, and users are made members of appropriate roles thereby acquiring the roles' permissions. In addition, roles can be granted new permissions, and permissions can be revoking from roles as needed. The significant benefit of deploying RBAC is its flexibility to meet the changing needs of an organization [5].

Privacy is a state or condition of limited access to a person [6]. In particular, information privacy relates to an

individual's right to determine how, when, and to what extent information about the self will be released to another person or to an organization [7]. In general, privacy policies describe an organization's data practices what information they collect from individuals (subjects), for what purpose the information (objects) will be used, whether the organization provides access to the information, who are the recipients of any result generated from the information, how long the information will be retained, and who will be informed in the circumstances of dispute. One can imagine that information privacy is usually concerned with the confidentiality of personal identifiable information (PII) and protected health information (PHI) such as electronic medical records. Though access control technology can be directly applied in protecting PII and PHI data, privacy concepts also have to be incorporated such as purpose and obligation. Threats to information privacy can come from insiders and from the outsiders in each organization [8]. Privacy control is usually not concerned with individual subjects. A subject releases his data to the custody of an enterprise while consenting to the set of purposes for which the data may be used [8]. The traditional view of access control model should be extended with an enterprise wide privacy policy for managing and enforcing of individual privacy preferences [9].

In this circumstance, the information access control mechanism should also be embedded with privacy-enhancing technologies [8]. All these evidences show the importance of integrating privacy concepts into access control mechanism for resolving the e-Healthcare security issues. The remainder of this paper organizes the discussion as follows. The next immediate section summarizes the relevant literature. With the context of e-Healthcare informatics, Section 3 proposes an extended framework of RBAC with privacy-based extension. Lastly, Section 4 concludes and future works.

2. Related Work

Today, privacy legislation in the U.S. (e.g., the HIPAA legislation) and in Canada (e.g., Bill C-6, Personal Health Information Protection Act) and strong industry standards adoption (ISO 17799) has led to heightened awareness of

privacy issues in e-Healthcare informatics. In the U.S., the Privacy Act of 1974 [10] requires that federal agencies grant individuals access to their identifiable records that are maintained by the agency, ensure that existing information is accurate and timely, and limit the collection of unnecessary information and the disclosure of identifiable information to third parties. In particular, the principle of information privacy and disposition requires that: All persons have a fundamental right to privacy, and hence to have control over the collection, storage, access, communication, manipulation and disposition of data about themselves [11]. Under the HIPAA privacy rules, protected health information (PHI) includes individually identifiable health information related to past, present, and future physical and mental health conditions, as well as the past, present, and future payment for the provisions of healthcare to an individual. HIPAA provided a set of standard policies that the healthcare providers have to exercise in order to protect a patient's privacy. In particular, privacy and confidentiality of information are closely related to security of e-Healthcare information use and distribution. Privacy technologies have been researched for a period of time [12]. However, there is still no standardized technology proposed yet.

In the e-Healthcare services context, security is only a matter of diligence in applying available tools to safeguard against potential risks. Today, many useful tools such as the ISO/IEC 17799 standard are available to formulate of a sound security framework. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) stipulate the characteristics of specialized systems for worldwide standardization. The ISO 17799 standard was published to provide an international framework for information security. The standard was not developed specifically for the healthcare industry; rather the scope of the document ensures cross-sector applications. Ten key areas that encompass a sound security framework are identified in the ISO 17799 standard with each section providing explicitly detailed protocols that meet the security associated with that area.

On the other hand, the family of Role-based Access Control (RBAC) developed by Sandhu et al. is commonly called the RBAC96 model [13, 14]. The RBAC96 model focuses on security control using roles and organizations. RBAC96 presents a conceptual model to describe different approaches such as base model, role hierarchies, constraint model and consolidated model. In particular, the National Institute of Standards and Technology (NIST) conducted market analysis for identifying RBAC features into two layouts: The RBAC Reference Model and the RBAC Functional Specification [15]. The RBAC Reference Model describes a common vocabulary of RBAC element sets and relations for specifying requirements and the scope of the RBAC features included in the standard. The

RBAC Functional Specification describes the requirements of administrative operations for creating and managing RBAC element sets and relations, and system functions for creating and managing RBAC attributes on user sessions and making access control decisions. In particular, the proposed RBAC model with privacy-based extension in next section is based on the core RBAC model discussed in [4]. Amidst other challenges, the most pressing privacy concerns that have observed for e-Healthcare informatics include: (1) the acquisition, storage, and processing of e-Healthcare data; (2) the consent to processing and disclosure of e-Healthcare data; and (3) the rights of the data subject (typically a patient for whom the data is being collected) to access and rectify his or her own health dataset [2]. Recently, Reid et al. present a RBAC for protecting privacy in distributed health care information systems with the concept of consent. In particular, the RBAC formulates the access control expressions as general denial with explicit consent [16]. Overall there is no concrete framework of RBAC with privacy-based extensions.

3. Propose the Role Based Access Control (RBAC) Model with Privacy-based Extensions

Traditional healthcare datasets housed within hospitals are mainly governed by a set of privacy regulations that determine the aim and scope of the registration, the type of data, the rights of data subjects, as well as access rights [17]. Access to e-Healthcare data should be just as securely protected. Yet, recent developments in e-Healthcare services will only deepen the conflict between individual privacy concerns and the pressure for health informatics from non-medical institutions (e.g., insurance companies) unless a rigorous security and privacy policy framework is developed [18]. For illustration, Figure 1 shows an e-Healthcare database application example involving three entities: Web Services Application, Web Service, and e-Healthcare Database. The Web services application can be any healthcare application at a health institute that is connected to a Web services at another health institute over the Internet. You can assume that the Web service is used as an interface to receive the request (e.g., retrieve/store health care data) from the application and then communicate with the e-Healthcare database at the backend (e.g., read/write data). Once the request is completed, the Web service returns a result (e.g., acknowledgement or health data) to the application.

Aside from the many reasons we have discussed, another reason security issues have to be studied and tackled seriously in e-Healthcare services is that the systemic use of protected health information (PHI) poses additional potential threats to the security, privacy, and confidentiality of e-patient information. For example, one

published survey reported that in the U.S., some people do not file insurance claims or see health service providers for fear that disclosure of their health information may hurt their job prospects or ability to obtain insurance coverage [18]. Note that a user can also belong to both the primary and the secondary user groups that may cause conflicts, for instance, a doctor can be a health service provider and an e-Healthcare informatics researcher. Additionally, of course, a patient may also be a doctor. As this section of the discussion focuses primarily on secondary e-Healthcare users, the term “users” refers specifically to secondary users unless explicitly specified otherwise.

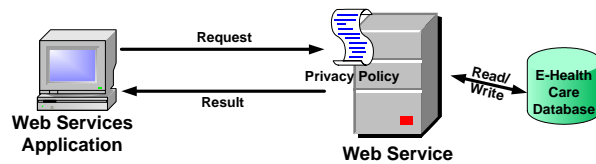


Figure 1. An Illustrative E-Healthcare Database Application Example

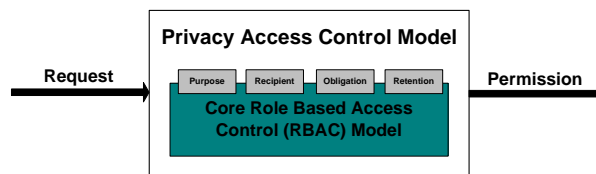


Figure 2. A Privacy Access Control Model

As you can see, the dynamic nature of e-Healthcare services makes information access control issues challenging. Thus, it has been proposed to implement RBAC to control user access to the information (i.e., datasets) held in the e-Healthcare services. The core RBAC is represented as a set of condition of use assertions in the context of users, roles, organizations, operations and datasets. In each data custodian, each user is belonging to an organization (e.g., hospitals) with at least one role (e.g., doctors) assigned. The roles can be classified as user roles or even administrative roles (e.g., security administrators). Based on the nature of roles, appropriate operations are assigned to roles for handling different jobs. For example, a “security administrator” role may be assigned with the operations of “assign users to roles,” and “assign permissions to roles.” Figure 2 presents an extended framework of core RBAC with privacy-based extensions. When a request arrives at the access control, the core RBAC is enhanced with the privacy-based extension (e.g., purpose, recipient, obligation and retention). Once the decision is made, either grant or deny the permission to the subject in according with the request, a set of obligations and a retention policy is also returned.

4. Conclusions and Future Work

Healthcare information might be considered the most intimate and personal information systematically collected and maintained about an individual. In most countries, e-Healthcare informatics is classified as sensitive information. This is because electronically stored data containing sensitive information can be easily and conveniently released, and disclosing sensitive information to outsiders can cause direct or indirect damage to an individual. Although security breaches have occurred in the era of paper records, the potential harm has been multiplied by electronic databases as information can now be transferred to a large number of people within extended boundaries. Imagine now that these various databases containing sensitive information are to be integrated and the combined aggregate data provided to a wide variety of users, including e-Healthcare practitioners, researchers, lawyers and business and government policy-makers [1]. It has been demonstrated that the use of a privacy access control model for e-Healthcare services will provide building blocks for secure and yet easy-to-access shared care systems. For example, information about e-patient medication is crucial for e-medical practice. Properly implemented medication e-registry systems are rare today and information is fragmented into several systems and organizations. E-Healthcare services will be invaluable both for planning e-patient treatment and research. The e-Healthcare service is therefore a good example of next generation client-centered e-Healthcare services that would be used among shared e-provider organizations [1].

Traditionally, secrecy provisions have protected privacy in healthcare. In general, organizational security together with password-based access control has been considered sufficient to protect patient data in medical information systems. This paper presents a framework of core RBAC with privacy-based extension. Extending RBAC model with privacy-based extensions by the inclusion of contextual authorizations increases the expressive power to define access control policies. Contextual information available at access time, like user/patient relationship, can influence the authorization decision that allows a user to perform a task. This enables a more flexible and precise authorization policy specification, where permission is granted or denied according to the right and the need of the user to carry out a particular job function [19]. With the e-Healthcare services context, one of our future works is to investigate an aggregation decision-making layer interacted with a set of autonomous RBAC models. With e-Healthcare services, security issues are much more complex as they involve aggregation of data and how conflicts of interest between users and the integrated view could be reconciled. We will look at different types of aggregation and the secrecy provisions to be enforced

along the content dimension.

Other future works include the realization of our proposed framework in a prototype to explore any potential usability and performance issues. In particular, the mechanisms and tools for managing the interactions taking place between different layers in the proposed framework. Privacy enforcement is a critical issue that needs to be addressed in urgent. While system interoperation with privacy enforcement using the ontology-based approach is promising in principle, more research effort and larger scale deployment are required in order for us to draw a more conclusive remark.

References

- [1] J. K. H. Tan and P. C. K. Hung, "E-Security: Framework For Privacy And Security In E-Health Data Integration And Aggregation E-Health Care Information Systems: An Introduction for Students and Professionals, Jossey-Bass - An Imprint of Wiley, pages 450-478, 2005.
- [2] F. France, "Control and use of health information: A doctor's perspective," *International Journal of Biomedical Computing*, vol. 43, no. 1-2, pages 19-25, 1996.
- [3] CSIS, "Security Glossary," Information Systems Security Organization, 2003. Online: http://ise.gmu.edu/~csis/glossary/merged_glossary.html
- [4] D. F. Ferraiolo, D. R. Kuhn and R. Chandramouli, "Role-based access control," *Computer Security Series*, Artech House Publishers, 2003.
- [5] S. Osborn, R. Sandhu and Q. Munawer, "Configuring role-based access control to enforce mandatory and discretionary access control policies," *ACM Transactions on Information and Systems Security (TISSEC)*, vol. 3, no. 2, 2000.
- [6] E. D. Schoeman, "Philosophical Dimensions of Privacy: An Anthology," New York, NY, Cambridge Univ. Press, 1984.
- [7] H. Leino-Kilpi, M. Valimaki, T. Dassen, M. Gasull, C. Lemonidou, A. Scott and M. Arndt, "Privacy: A review of the literature," *International Journal of Nursing Studies*, vol. 38, pages 663-671, 2001.
- [8] S. Fischer-Hubner, "IT-Security and Privacy," *LNCS* 1958, 2001.
- [9] C. S. Powers, P. Ashley and M. Schunter, "Privacy promises, access control, and privacy management - Enforcing privacy throughout an enterprise by extending access control," *Proceedings of the Third International Symposium on Electronic Commerce*, pages 13- 21, 2002.
- [10] J. C. Davis, "Protecting privacy in the cyber era," *IEEE Technology and Society Magazine*, pages 10-22, Summer 2000.
- [11] HL7, "HIPAA Claims and Attachments Preparing for Regulation," May 2004. Online: www.hl7.org/memonly/downloads/Attachment_Specifications/HIPAA_and_Claims_Attachments_White_Paper_20040518.pdf
- [12] V. Senicar, B. Jerman-Blazic and T. Klobucar, "Privacy-enhancing technologies – approaches and development," *Computer Standards & Interfaces*, Volume: 25, Pages: 147-158, 2003.
- [13] R. S. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman, "Role-based access control models," *IEEE Computer*, Volume: 29, Number: 2, Pages: 38-47, 1996.
- [14] R. S. Sandhu, V. Bhamidipati and Q. Munawer, "The ARBAC97 model for role-based administration of roles," *ACM Transactions on Information and Systems Security (TISSEC)*, Volume: 1, Number: 2, Pages: 105-135, 1999.
- [15] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn and R. Chandramouli. "Proposed NIST Standard for Role-Based Access Control," *ACM Transactions on Information and Systems Security (TISSEC)*, Volume 4, Number 3, 2001.
- [16] J. Reid, I. Cheong, M. Henriksen and J. Smith. "A Novel Use of RBAC to Protect Privacy in Distributed Health Care Information Systems," *Proceedings of the Eighth Australasian Conference on Information Security and Privacy (ACISP 2003)*, LNCS 2727, pages 403-415, 2003.
- [17] K. Louwerse, "The electronic patient record; the management of access—case study: Leiden University Hospital," *International Journal of Medical Informatics*, vol. 49, no. 1, pages 39-44, 1998.
- [18] J. Anderson, "Security of the distributed electronic patient record: a case-based approach to identifying policy issues," *International Journal of Medical Informatics*, vol. 60, no. 2, pages 111-118, 2000.
- [19] G. H. M. B. Motta and S. S. Furuie, "A contextual role-based access control authorization model for electronic patient record," *IEEE Transactions on Information Technology in Biomedicine*, vol. 7, no. 3, pages: 202- 207, Sept. 2003.

Acknowledgements

This research is partly funded by a discovery grant (NSERC PIN: 290666) from the Natural Science and Engineering Research Council (NSERC) of Canada.