Research Issues of Privacy Access Control Model for Mobile Ad Hoc Healthcare Applications with XACML

Patrick C. K. Hung[1], Jude Andrade[1], Yongming Chen[1], Ranny Huang[1]
Miguel Vargas Martin[1], Yi Zheng[12]
[1]Faculty of Business and IT, University of Ontario Institute of Technology (UOIT), Canada
[2]Department of Computer Science, Technical University of Munich, Germany
{Patrick.Hung, Miguel.Vargas-Martin}@uoit.ca
{Jude.Andrade, Yongming.Chen, Haoran.Huang}@mycampus.uoit.ca; zheng@in.tum.de

ABSTRACT

Information privacy is usually concerned with the confidentiality of protected health information (PHI) such as electronic medical records (EMR). To meet the needs of highly mobile patients in healthcare scenarios, mobile devices such as personal digital assistants (PDAs) are being used for storing entire patient histories and physicals, research data collection forms, the physician's reference desk, current care plans, and drug orders. Thus, the information access control mechanism for mobile ad hoc healthcare applications must be embedded with privacy-enhancing technologies. This paper presents the research issues of developing a privacy access control model for supporting mobile ad hoc healthcare applications. This paper also shows how eXtensible Access Control Markup Language *(XACML) can protect confidential EMR in such a setting.*

Keywords: XACML, Role Based Access Control, Privacy, mobile ad-hoc network, Healthcare Applications.

1. INTRODUCTION

Protected health information (PHI) includes individually identifiable health information and the provision of healthcare to an individual relating to past, present, and future physical and mental health conditions. Compromises to the PHI in healthcare systems can seriously affect patients' health and may be life threatening. It may adversely affect a patient's diagnosis or treatment, resulting in misdiagnosis, delaying treatment, or providing the wrong treatment. Leakage of PHI might not only potentially create personal embarrassment; it could also lead to social ostracism. More dire consequences include denial of insurance coverage, loss of job opportunities, and the refusal of mortgage financing [9]. With the introduction of the electronic medical records (EMR) into the healthcare sector, PHI has been made available via electronic means to a wide range of medical personnel such as nurses and specialists.

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. Role based access control (RBAC) is a system of controlling which users have access to resources based on the role of the user. The access rights are grouped based on the role name and access to resources are restricted to the users who have assumed a specific role. For example in a hospital, individuals who were allowed on the network would be assigned a predefined role (e.g., physician, nurse, lab technician, and administrator). Based on the role assigned to them, individuals would only be able to carry out actions defined by their role. For example, a physician would only be able to access resources on the network that the role of "physician" has been allowed access to. Each user can be assigned more than one role, and each role is assigned one or more privileges to users in that role [1].

Privacy is a state or condition of limited access to a person (e.g., patient) [10]. 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 [11]. 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 PHI. Though access control technology can be directly applied in protecting PHI data, privacy concepts also have to be incorporated such as purpose and obligation. 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 [12]. The traditional view of access control model should be extended with an enterprise wide privacy policy for managing and enforcing of individual privacy preferences [13].

In mobile ad hoc healthcare scenarios, the information

21st International Conference on
Advanced Information Networking and Applications Workshops (AINAW'07)
0-7695-2847-3/07 $20.00 © 2007 IEEE

access control mechanism should also be embedded with privacy-enhancing technologies [12]. The paper will look at the various privacy issues for each healthcare stakeholder to access EMR involved with the use of mobile ad-hoc network (MANET) in a hemodialysis scenario. We consider collaboration among a group of individuals each supported by a mobile device such as personal digital assistants (PDAs). The individuals (and their devices) come together on an ad hoc basis in the sense that their devices had not been programmed a priori to work with each other. We assume the interactions take place when the individuals are in close proximity, e.g., face-to-face. This paper presents the research issues of developing a privacy access control model for supporting mobile ad hoc healthcare applications. In particular, this paper also discusses how eXtensible Access Control Markup Language (XACML) can protect confidential EMR in such a setting. The remainder of this paper is organized as follows: Section 2 presents the research issues of mobile access control model for supporting mobile ad hoc healthcare applications with XACML. Next, Section 3 presents a proof of concept implementation. Section 4 concludes the paper with future works.

2. RESEARCH ISSUES OF MOBILE PRIVACY ACCESS CONTROL MODEL

In this paper, we refer to privacy based on the following principle for protecting PHI in healthcare applications [16]:

- Principle 4: Limitation principle
  - Limitation on Collection: The collection of PHI shall be limited to specific legitimate purposes of collection only. For example, a doctor can access his/her patient's PHI for treatment purpose and the collected PHI should be used for treatment only.
  - Limitation on Disclosure: The owner of PHI should be able to make special restrictions on the disclosure of his/her own PHI. For example, a PHI owner can restrict his/her own PHI not to disclose to any third-party for marketing purpose.
  - Limitation on Use: The use of PHI shall be identified as legitimate use by the services provider and/or the owner of PHI. For example, a doctor uses his/her patient's PHI for treatment purpose is a legitimate use.
  - Limitation on Retention: PHI shall be retained for only as long as the purpose for which it is used.

This research is fallen into the category of distributed intermediary in privacy-enhancing technologies, which rely on the cooperation of many distinct intermediaries [21]. The use of mobile devices in healthcare can be used in the form of an ad hoc network to aid in the transfer and accuracy of PHI. This paper focuses on the privacy issues in the use of technology in a healthcare setting, through the means of MANET. MANET is based on a self-organizing and rapidly deployed network of mobile devices to exchange information without using any pre-existing fixed network infrastructure, such as in the patient's home and emergency response situation. The MANET provides an infrastructure-less environment for supporting mobile devices with a viable means of transferring EMR to any necessary healthcare practitioners [14]. In order to accomplish a theoretical privacy access control model for handling mobile ad hoc healthcare applications in the Services Oriented Architecture (SOA), the privacy properties of SOA [17] and the following five fundamental mobile ad hoc properties that the model must meet [15] have to be implemented:

1. *Mobility*: Mobile devices should only be limited by the range, which is set by the business logic of the application.
2. *Peer-to-Peer*: Mobile devices have to interact and communicate directly with each other, without using a central server.
3. *Collocation*: All logical interactions between applications have to result in a physical interaction between location-based users.
4. *Collaboration*: Collocated mobile devices need to be willing to collaborate.
5. *Transitory Community*: Mobile devices/users may join and withdraw from the interactions at any time, making it an ever changing map.

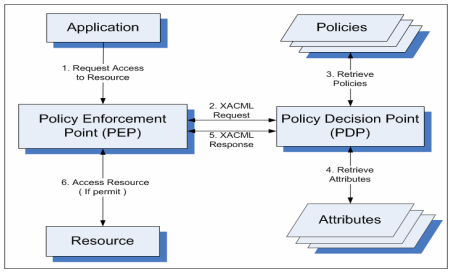

Figure 1. XACML Policy Enforcement and Decision Model [22]

As the privacy access control enforcement model is built in supporting the interactions of mobile devices, we have to look into an abstract model for policy enforcement defined by the Internet Engineering Task Force (IETF) [23]:

- *Policy Decision Point (PDP)*: The point where policy decisions are made.
- *Policy Enforcement Point (PEP)*: The point where the policy decisions are actually enforced.
- *Resource*: Something of value in a network infrastructure to which rules or policy criteria are first applied, before access is granted. This can be referred as

the objects in the privacy access control model.

- *Policies*: The combination of rules and services where rules define the criteria for resource access and usage. This can be referred to as the privacy rules in the privacy access control model.

The privacy access control enforcement model can use this abstract model as the base of technical framework. However, this abstract model does not consider any privacy entities in mobile ad hoc applications. Thus we have to build a new enforcement model for tackling the mobile ad hoc healthcare applications. XACML has been standardized by Organization for the Advancement of Structured Information Standards (OASIS) [2]. XACML's syntax is defined in XML, and describes both an access control policy language and an access control decision request/response language. The access control requirements are described by the policy language, while the request/response language allows a query to be formed to ask whether or not a given action should be allowed, and interpret the result [3]. XACML allows administrators to define access control requirements for the application resources [4].

Figure 1 shows the interaction between different components in the XACML policy enforcement and decision model as follows: (1) First, the application requests for access to a resource at the PEP; (2) After gathering the necessary information, the PEP formulates an XACML request and sends it to the PDP; (3) The PDP fetches the necessary policies; (4) Necessary attributes for decision making; (5) After determining a decision, the PDP returns an XACML response back to the PEP; and (6) The PEP then enforces the decision by allowing or denying access to the resources. The privacy access control model can use this as its policy enforcement and decision model. The application and the PEP represent a subject that makes a request to access an object (resource). The policies, the PDP and the attributes are representing the privacy rules, access control algorithms, and the extended entities respectively in the privacy access control model.

A request must demonstrate the access control requirements specified by the policy language in order for the user (requester) to be granted access. A typical XACML model has certain entities that protect resources and verify users privileges based on access control policies. When a user tries to perform an action on resource, their query is received by the entity that protects the resource. This entity is known as the PEP and it is responsible for protecting the resource from any unauthorized access. The PEP is not responsible for evaluating the requestor's information; instead it creates an XACML request based on the attributes of that user, the desired action, the resource, and the properties of the environment at the time of the user query. The PEP forms a request (using the XACML request language) request to the modular PDP, which may or may not be located on the same local network [6]. The PDP then examines the request, retrieves policies (written in the XACML policy language) that are applicable to the request, and determines whether access should be granted. The answer (expressed in the XACML response language) is then returned to the PEP which will enforce the decision, to allow or deny access to the requester [2]. It must be noted that XACML does not make decisions, but rather gives a response according to the policy input it receives [8].

3. PROOF OF CONCEPT IMPLEMENTATION

There are major reasons for adopting mobile technologies in healthcare such as to improve the healthcare quality at point of care, reduce cost, and increase achievement efficiencies. In this context, security and patient privacy is always a major issue for both practitioners and patients in adopting mobile technologies. The Canada Health Infoway (CHI) suggests that mobile and wireless technologies with privacy protection are needed to maintain a high-quality, sustainable and effective Canadian health care system. For instance, in emergency response situations, the ability to access an EMR effectively and reliably in a mobile environment will be an extra-positive advance. Recent changes in federal (e.g., FIPPA, PIPEDA and PHIPA) and provincial legislation have created a tremendous gap between current privacy processes and technology. Thus, the effective and timely support of mobile devices computing security and privacy model will become very important to the healthcare sector in Canada.

In order to show the preliminary idea of this research to the healthcare research community, we have developed a preliminary proof-of-concept demonstration based on the healthcare settings of the hemodialysis process. The nature of hemodialysis suits the healthcare settings with mobile devices and highlights the privacy concerns. The hemodialysis process is an asynchronous cooperation between the visiting nurses over a long period of time, with many temporal ruptures. Data about the hemodialysis process were obtained from patient records that are kept in the patients' homes (mobile devices) and are updated by the nurses after every visit [26]. Referring to Figure 2, the prototype consists of two sets of equipments in two settings: *Patient's Home* and *Hospital*. In the patient's home, there are: (a) *Dialysis Server*: It is a simulated dialysis machine with database at the patient's home which has BlueTooth connectivity to the patient's PDA. To store EMR, we use SQL server to simulate the Medi-Tech Server which is widely used in the healthcare sector; (b) *Patient and Nurse PDA*: They are the mobile devices which the patient and nurse are holding at his/her hand at the patient's home. These PDAs also have the BlueTooth

connectivity to the dialysis server and each other with SQL Mobile to store EMR; and (c) *Nephrologist Smartphone*: This is the future work of this research. Basically this smartphone will form a MANET with the nurse and patient PDA. In the hospital, the nurse brings back her PDA and connects to the Web service server in the hospital to upload the EMR via WiFi connectivity. On the other side, the doctor can view the EMR uploaded by the nurse via WiFi connectivity as well.

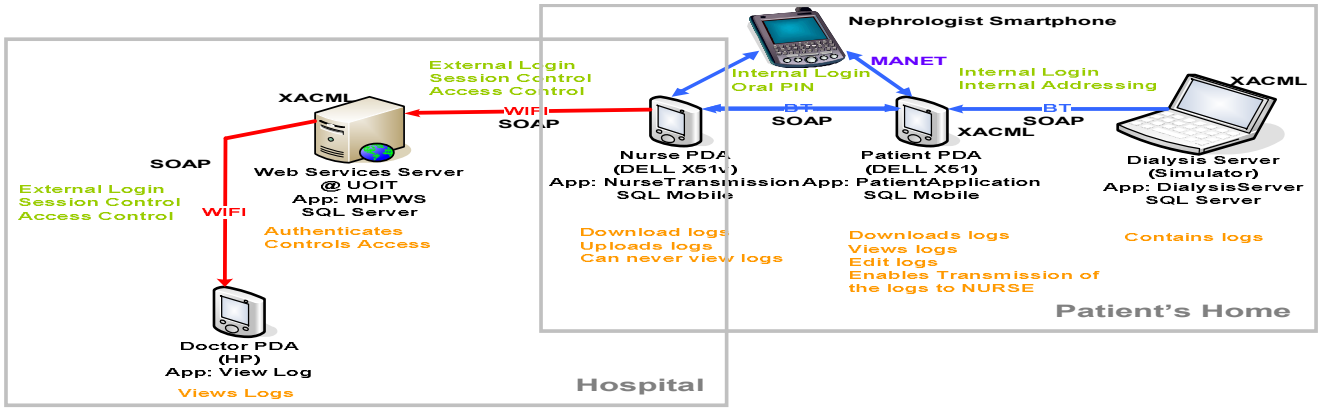

Figure 2. Preliminary Proof-of-Concept Prototype Settings

To our best knowledge, there is still no privacy access control component being discussed in this emerging research community, and this research component is particularly important for supporting business applications in MANET computing [27]. Therefore this project is one of the first to explore in this challenging new research area. Beside XACML, there is another major emerging standard adapted in this prototype: Simple Object Access Protocol (SOAP). SOAP is an XML-based messaging protocol that is independent of the underlying transport protocol. SOAP messages are used both by services requestors to invoke Web services, and by Web services to answer to the requests. Therefore, the Web service receives the input SOAP message from the Web services requestor and generates an output SOAP message to the Web services requestor [7]. All the messages exchanged between the devices in the prototype are formatted in SOAP.

Based on this setting, we are currently investigating a few scenarios. Referring to Figure 3, a nurse is attempting to communicate with the patients PDA. The communication between the nurse and patient will be direct device-to-device (peer-to-peer). We will refer to the nurse PDA as "PDA-N" and the patients PDA as "PDA-P." In this scenario, the nurse is attempting to obtain the information from a home hemodialysis patient's PDA who is considered the owner of the resource/information (data on the PDA). Since the PDP is responsible for protecting the resource/information on a device, it would be located on the patient's PDA in this scenario. The PEP would be on the service requestor side and would be located on "PDA-N" who is requesting to download the patient's diary. The patient's PDA will also contain the relevant policies to enable the PDP to make the authorization decision. The policy in this scenario would contain rules that would allow the nurse the authority to download the patient's diary log.

When the nurse tries to access the patient's PDA the PEP sends a request using the XACML request language based on the attributes of the subject, action, resource and other relevant information. This information is received by the PDP which compares the request from the PEP to the applicable policies. Based on the input it receives from the policy, the PDP will send a "*Permit*" or "*Deny*" decision back to the PEP. The PEP will then enforce the decision and either permit access to the nurse if she has the proper authorization or deny access to the nurse if she does not have the proper authorization.

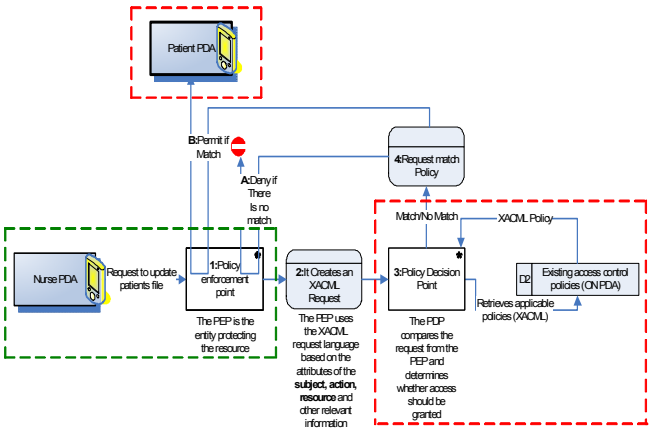

Figure 3. XACML Decision Logic in the Prototype

In this example, a central database server (e.g., Medi-

tech server) will be the storage point for the patient's information in the hospital. The nurse will upload the EMR from his/her PDA to the Medi-tech server once at the hospital. Similarity, the nurse will only be allowed to upload the information if he/she has the proper authorization. In this scenario, the PEP and PDP can be both located on the Medi-tech server. The PEP will create a request, which will be used by the PDP to retrieve the applicable policies. Based on the policy, the nurse will be granted or denied access to update the patient's health data. In the same manner, a doctor can access the Medi-tech server from their PDA to view the patient's health records, if they have the proper authorization.

In this example, a nephrologist is attempting to communicate to a patient/nurse in an ad hoc situation, e.g., emergency response. The communication between the nephrologist and the patient/nurse will be in indirect device-to-device. In this mode, the distance between the two nodes (mobile devices) is much greater than the BlueTooth connectivity can handle. Thus this situation requires the assistance of other nodes to communicate. Instead of communicating directly with the desired PDA, the request/response and the exchange of data is made possible by the presence of other nodes. The nodes will act like routers and pass any requests/response or data to the target node when information is sent out. This allows communication between mobile devices far beyond the usual reach of installed infrastructure. This is the simplest infrastructure of a MANET for supporting the roaming mode. Referring to Figure 4, there are three roaming scenarios shown as follows:

- *Roaming Scenario #1*: The nurse is downloading information from the patient's PDA. Since the PDP protects the data it will be located on the patient's PDA while the PEP which enforces the decision will be on the nurse's PDA.
- *Roaming Scenario #2*: The nephrologist is downloading information from the nurse's PDA. Similar to the last scenario, the PDP will now be located on the nurse's PDA since it now contains the private data. The PEP will be located on the nephrologist's PDA to enforce the decision.
- *Roaming Scenario #3*: The nephrologist could download the information directly from the patient's PDA. In this scenario, the PEP will be located on the nephrologist's PDA while the PDP will be on the resource it is protecting, the patient's PDA.

Furthermore, another healthcare example that could benefit from roaming mode could take place between the nephrologists and the medical supplier. If a change of medication was required, the nephrologists could request to change the medication recorded in the patient's EMR. The patient or the medical supplier in another location could then request to view the updates to the medication. This communication could take place without any existing network infrastructure and would eliminate the need for the patient to go to the hospital to pick up a new prescription.

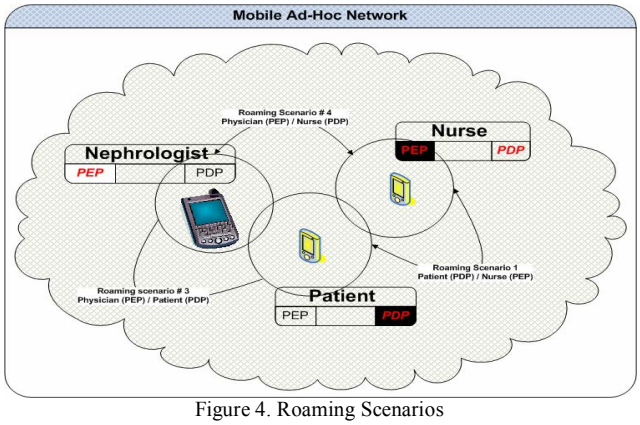

Figure 4. Roaming Scenarios

4. CONCLUSIONS AND FUTURE WORKS

In this paper, we present the research issues of developing a privacy access control model for supporting mobile ad hoc healthcare applications. This is only a preliminary concept of this research work. In particular, the major research challenge is that the mobile devices come together on an ad hoc basis in the sense that the devices had not been programmed a priori to work with each other. We also believe that the model does not have to be limited to the healthcare sector. The methodology can also be adopted into other MANET computing scenarios such as natural disaster communications (e.g., tsunami, earthquakes), emergency relief scenarios, car-based networks, and the provision of wireless connectivity in remote areas. Referring to Beneteau and Orsini [24], the major barrier that is preventing most of the hospitals in Canada from adopting emerging technologies in new and innovative ways is the need for a secure medium to exchange information and privacy standards to ensure patient information remains confidential. The privacy access control model should provide the assurance that designed safeguards for handling PHI are compliant with privacy legislation and data protection principles, such as FIPPA, PIPEDA, and PHIPA. In this research work, XACML will be the first emerging technology we investigate to be one of the starting points to fill into the picture [25]. The future works include: (1) Design a systematic methodology to link management-level privacy considerations and objectives in the context of MANET healthcare services; (2) Build the theoretical vocabulary independent model of privacy access control for mobile ad hoc healthcare applications with view management, communications and ontology; and (3) Develop the technical framework of privacy access control enforcement for mobile ad hoc healthcare applications

extended from the abstract model for policy enforcement defined by the IETF.

ACKNOWLEDGEMENT

This work was supported in part by research grants (NSERC PIN: 290666) from the Natural Science and Engineering Research Council (NSERC) of Canada and Bell University Lab (BUL). Special thanks to Ms. Stephanie Chow at UOIT for her great effort and help in improving the presentation of this paper.

REFERENCES

[1] 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.

[2] Sun Microsystems, "Sun's XACML Implementation," Sun's XACML Implementation, 2004.

[3] Sun Microsystems, "Sun's XACML Implementation Programmers Guide," Sun's XACML Implementation, 2004.

[4] P. Griffin, "Introduction to XACML," Developers, 2004.

[5] I. Mavridis, C. Georgiadis, G. Pangalos and M. Khair, "Access Control Based on Attribute Certificates for Medical Intranet Applications," Journal of Medical Internet Research, vol. 3, no. 1, 2001.

[6] P. Mazzuca, "Access Control in a Distributed Decentralized Network: an XML Approach to Network Security Using XACML and SAML" Dissertation, Darthmouth, 2004.

[7] W3C, "SOAP version 1.2 Part 0: primer. (W3C Recommendation)," World Wide Web Consortium (W3C), June 2003.

[8] J. Wu and P. Periorellis, "Authorization-Authentication Using XACML and SAML," School of Computing Science, e-Science Centre, Newcastle University. Newcastle, 2005.

[9] 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, pp.450-478, 2005.

[10] E. D. Schoeman, "Philosophical Dimensions of Privacy: An Anthology," New York, NY, Cambridge Univ. Press, 1984.

[11] 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.

[12] S. Fischer-Hubner, "IT-Security and Privacy," LNCS 1958, 2001.

[13] 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.

[14] A. A. Pirzada and C. McDonald, "Establishing trust in pure ad-hoc networks," Proceedings of the 27th conference on Australasian computer science (CRPIT '04), Volume 26, Pages 47-54, 2004.

[15] B. Garbinato and P. Rupp, "From ad hoc networks to ad hoc applications," Proceedings of the 7th International Conference on Telecommunications (ConTEL 2003), Volume 1, Pages 145-149, 2003.

[16] V. S. Y. Cheng and P. C. K. Hung, "Privacy principles for developing multi-legislation compliant e-healthcare Web services applications," Proceedings of the Fourth Workshop on e-Business (WeB 2005) in conjunction with the International Conference on Information Systems (ICIS 2005), 12 pages (CD-ROM), 2005.

[17] W3C, "Web Services Architecture Requirements," World Wide Web Consortium (W3C) Working Draft, 14 November 2002.

[18] W3C, "The Platform for Privacy Preferences 1.0 (P3P1.0) Specification," World Wide Web Consortium (W3C) Recommendation, 16 April 2002.

[19] HL7, "HIPAA claims and attachments preparing for regulation," May 2004.

[20] W3C, "SOAP Version 1.2 Part 1: Messaging Framework," World Wide Web Consortium (W3C) Proposed Recommendation, 07 May 2003.

[21] I. Goldberg, "Privacy-enhancing technologies for the Internet, II: Five years later," Zero-Knowledge Systems, Inc., 2006.

[22] OASIS, "eXtensible Access Control Markup Language v2.0 Core (XACML)," OASIS, 2006.

[23] R. Yavatkar, D. Pendarakis and R. Guerin, "A framework for policy-based admission control," IETF RFC 2753, January, 2000.

[24] L. Beneteau and S. Orsini, "eHealth - The Emerging Frontier in Health Care," 2005.

[25] V. S. Y. Cheng, and P. C. K. Hung, "Health insurance portability and accountability act (HIPAA) compliant access control model for Web services," The International Journal of Health Information Systems and Informatics (IJHISI), Volume 1, Issue 1, pp. 22-39, 2006.

[26] S. Hamek, Anceaux, F., Pelayo, S., Beuscart-Zéphir, M.C. and J. Rogalski, "Medical applications: Cooperation in healthcare - theoretical and methodological issues: a study of two situations: hospital and home care" Proceedings of the 2005 annual conference on European association of cognitive ergonomics (EACE '05), Pages 233-240.

[27] U. Varshney, "Using Wireless Networks for Enhanced Monitoring of Clients," Proceedings of the Tenth Americas Conference on Information Systems, 7 pages, 2004.