Sindh Univ. Res. Jour. (Sci. Ser.) Vol.44 (2)197-202 (2012)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

State-of-the-art in eHealthcare Security and Privacy

M. MEMON, A. KEERIO*, J. A. MAHAR**, Z. HUSSAIN***, M. HYDER, G. D. MENGHWAR

Information Technology Center, Sindh Agriclture University, Tandojam, Pakistan

Corresponding Author: ayazkeerio@hotmail.com Cell No. +92 3412802830

Received 13th December 2011and Revised 27th April 2012

Abstract: The patients' medical records contain sensitive information of the individuals, whose unwanted disclosure may harm their personal life. In the e-Healthcare environment, medical records are distributed and shared among various medical and non-medical organizations. This creates problems in providing sufficient confidentiality and integrity to the medical data. As a result, security and privacy of patients' data becomes more complex in today's decentralized, loosely-coupled and service-oriented systems. This paper presents various application models and architectures that provide security and privacy to patients' personal and medical data in eHealthcare Systems. The models are applicable to healthcare services to ensure security and privacy to users' data and give control of the data to the authorized users of the medical organizations based on the organizations policies and privacy preferences of the patients.

Keywords: eHealthcare personal and medical security.

1. INTRODUCTION

With the wide and rapid worldwide deployment of Internet and telecommunication technologies in our daily life new generation of eServices like eGovernment, eCommerce, eEducation and eHealthcare services have taken over the legacy web applications. One very critical aspect of such eServices is to provide security and privacy to users' data, while they access the services, which are distributed with intricate application architectures across heterogeneous platforms and communication technologies using vulnerable and hostile medium of Internet for sharing the sensitive data. The medical records may contain the sensitive information of the individuals whose unwanted disclosure may harm their personal life as those contain an individual's data of psychological and sexual disorders, genetic dispositions and emotional problems etc. The user visualizes the privacy at different levels of perception of information security; for example a user would like to enforce more strict privacy on the medical records as compared to the educational records. The user's perception also depends upon the many factors such as receiver of information and its use (Dritsas, Gymnopoulos2, *et. al,* 2006).

In the eHealthcare services, the patients' data is shared among various collaborating partners to provide timely access to the medical record of patient and provide authorized access to the legitimate user of the system to guarantee better quality of health services (Goldberg, and Brewer, 1997). The partners with diversified interests access the medical data using different communication technologies and security domains, therefore providing security and confidentiality of patient data becomes more complex in such situations. Moreover, when users interacting with composed services enter the identification information, it is also difficult to maintain and verify their digital identity (with authorization) at different partners' end.

2. MATERIAL AND METHODS

Security and Privacy Requirements of Medical Data

According to social requirements, which are depicted in the legal specifications, security and privacy of citizens' medical records is a very sensitive issue. Most of the legislation entitles the citizen as the owner of her medical data and provides her more rights than anyone else on her medical records. This implies that it is mandatory to get consent from citizens, when her medical records are accessed for any purpose.

The current situation clearly portrays the severity and seriousness of security and privacy problems in the eHealthcare systems (Ryen. Doyle, 2008; Peel, 2010). The question is how to achieve security and should the citizens in today's digital world rely on the security infrastructure of enterprises, which handle their personal and medical data? Generally, the medical records are accessed for two purposes. The primary purpose is to provide timely healthcare services to the patient. For that, different roles in healthcare organizations access the medical data. For example, a primary physician at clinic or hospital would access the

*University of Sindh, Jamshoro, Pakistan
**Department of Computer Science, Shah Abdul Latif University, Khairpur, Pakistan
***Quid-e-Awan University of Engineering, Science and Technology, Nawabshah, Pakistan

Patient's Medical Record (PMR) to give her treatment for a disease. Moreover, she may refer the patient to a specialist for further diagnosis of the disease through radiography. The Radiography Specialist in the diagnosis lab would access the referral sent by Primary Physician. Moreover, she needs to access patient's medical history to conduct the diagnosis tests on patient.

In a simple scenario like this and even in more complex scenarios, there are a number of requirements concerned with security and privacy of PMRs. In the simplest case, different users in healthcare organizations such as Clinic, Diagnosis Lab, Pharmacy and Insurance are assigned certain roles based on their organizational responsibilities. This prevents from un-authorized access to medical data. The roles use eHealthcare services and are identified based on the credentials assigned to them such as digital certificates and logins. The roles have defined permissions for accessing medical services. The permissions are defined in the authorization policies for those roles. Another complex healthcare-specific scenario worth-mentioning here is the access to medical data in *Emergency Situations*. In emergency, access restrictions or permissions should be over-ruled to give an un-restricted access to an emergency doctor or surgeon, who attends the citizen. In this context, when a patient cannot give consent due to an accident, then her legal- or family- representative can give consent instead of her. So that the surgeon may refer the affected patient's medical record and provide her timely treatment (Kuenzi, *et. al.,* 2009; Becker, 2005). For example, in case of a heart-attack emergency, a cardiologist needs the history of patient's previous heart attacks and the medicine previously consumed by her. From the medical records, an emergency doctor may notice if the patient has some allergies from some type of medicine, then she should avoid prescribing such medicine. However, the access to medical records in case of emergency should ensure *Auditing,* which means that if a surgeon has accessed the medical data of a patient un-restrictively in emergency situations, then she should not be able to misuse the short-time privileges given to her. Auditing is achieved with Non-repudiation, which produces irrefutable evidences generated by the security protocols, so that the same can be used for auditing.

Other than the primary use of medical data, which is precisely for the treatment of citizens, the medical data is also used for *Secondary Purposes* (Lowrance, 2003; Emam, 2006). The secondary use of patients' medical records is performed by the organizations, which are involved in medical research, survey or academics. This is very important for knowledge contribution to do research on the medical data to know a number of facts and figures about diseases, medicines and other sociological factors. The outcomes of such research are used for the improvement and evaluation of medicines, medical practices and medical equipment/technologies etc. The statistics collected from the research are also used for social research, which helps governments formulate policies and strategies to solve public health problems.

From the secondary use perspective, the citizen's medical records contain two types of information. The first type of information is concerned with the identity of the patient. This part is known as Personal Identifiable Information (PII) (P. C. K. Hung, 2005). PII could be the name, address, social security number, telephone number or any other information related to an individual's identity. The other information that is an essential part of the medical records is the medical history containing the information about diseases, medicines prescribed, effect of medicines, diagnosis tests, and radiography images (e.g., X-Ray, Ultrasound images etc.). This part of the medical records is the prime input of medical research. If only this information is released from hospitals to research organizations without PII, using anonymization techniques, then it is not easy to identify an individual. By hiding the PII part of medical record, the citizens' privacy can be preserved using certain anonymization techniques. Moreover, it is also debatable if the secondary use of medical data requires the consent from the citizen or not? This is a very interesting issue elaborated in (Lowrance, 2003).

Above discussion leads us to the point, that security requirements of healthcare systems are very distinctive and complex due to sensitivity of medical data. To achieve those requirements, the policies defined by eHealthcare organizations should conform to the legislation formulated by the concerned authorities. Extensive academic and industrial research has addressed healthcare security and privacy concerns, from legal and technical point of views. Some of the prominent research is briefly presented in the Related Work section.

3. Background And Related Work

There is lot of research work in the area of healthcare security and privacy focusing legal, organizational, social and technical aspects.

(Yee, and Korba, *et. al.,* 2006) suggest a control over the identification information in the hands of the user and distribute it only on a need-to-know basis. According to (Emam, 2006), researchers are increasingly turning to Electronic Medical Records (EMRs) to collect research data from usual practice. The ease of storage and exchange of large volumes of health data electronically has raised privacy issues. He further investigates the use of anonymization techniques when medical data is used for research. According to his research, there is a need of "Strong Privacy Expertise" to educate the data collectors, about how to practice anonymization effectively. (Annas, 2002) has investigated the federal regulations for privacy and

claims that those are not appropriately designed to allow access to healthcare research. This raises many reservations from the medical industry and academics. According to research institutions the regulations will make it more difficult, if not impossible, to conduct research involving the use of medical records. The research addresses the secondary use of medical data, which is an important issue in the healthcare security and privacy, as investigated by (Lowrance, 2003).

Furthermore, (Dimitropoulos, *et. al.,* 2007) have highlighted some very interesting solutions for interoperable health information exchange. Citizen's consent for accessing her medical data is yet another indispensable issue regarding healthcare security and privacy. (Win and Fulcher, 2007) believe that due to abuse of medical data the healthcare providers avoid integration of healthcare applications, despite great benefits. (Rannenberg *et. al.,* 2009) have discussed the identity management issues for citizens of European Union for different sectors including health to secure their sensitive health data. In a technical report, (Becker, 2005) has investigated the development of a UK-based EHR architecture with technical and organizational issues challenges regarding security and confidentiality of patients' identification medical data. The formal authorization policy, described by them considers the main aspects such as access control of patients' identification data, legitimate relationships, patients' restricting access, authenticated and third party consent.

(Hafner, *et. al.,* 2006) have addressed the high-level system design and low-level architectural and technical issues related to real world healthcare security problems. They suggest defining high-level security and privacy policies in the eHealthcare business processes and designed a reference architecture realizing those requirements. (Hung, 2005; Hung, *et. al.,* 2007) have proposed a Privacy Access Control Model for e-health systems based on HIPAA regulations. They have developed a privacy access control model for ad-hoc network-based eHealthcare mobile applications. According to them, accessing medical data through seamless WLAN-based hotspots poses security challenges (Mitseva, *et. al.,* 2006).

Citizen's control over their own medical data is a potential topic in healthcare privacy. (Kuenzi, *et. al.,* 2009) have characterized the issue of accessing medical records in emergency conditions. While, user-managed access policies realizing ownership of healthcare records are discussed by (Chinaei and Tompa, 2005). They have proposed a distributed authorization system to allow a corporate policy for all health record owners to administer access control over their data objects. The toolset proposed by (Blobel and Roger-France, 2001) mainly focuses the Design, Implementation and Maintenance of distributed secure health information systems manageable. Their *Concepts-Services-Mechanisms-Algorithms* view refines high-level security requirements to implementable technologies. (Li, and Poovendran, 2005) and (Alam, *et. al.,* 2007) have discussed the *Rights Delegation* issues in eHealthcare systems to restrict access by a user, who is not the primary care physician of the citizen.

4. STATE-OF-THE-ART IN Ehealthcare SECURITY AND PRIVACY

This section discusses the state-of-the-art in eHealthcare Security and Privacy in the perspective of security controls and architectures used for data confidentiality and integrity.

4.1 ACCESS CONTROL

The fundamental requirement of providing the security is the authentication and authorization services. Authentication ensures that only legitimate user with appropriate digital signatures enters the eHealthcare System, whereas the authorization is responsible to ensure that the users access the resources based on the permissions given to them which are based upon their roles and enforced by the policies.

Various Access Control models such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-based Access Control (RBAC) and Context-aware Access Control (CAAC) provide the authorized users access to the system resources and functionalities for the eHealthcare System Scenarios. The authentication and authorization may be comprehended in more depth in the eHealthcare Systems with following requirements and their corresponding solutions.

a) A Physician at the hospital using clinical information system with his digital signature is authorized to access the medical history of patient, add specialist(s) to Access Control List and add /modify prescription.

b).A Physician can delegate his access rights to a surgeon or specialist, who can further add other specialist(s) in the access control list for patients' references.

4.2 EMERGENCY ACCESS

In case of Emergency or life-threatening situations the Break-glass approach may be adapted where conventional Access Control Policies may be overruled so that the attending doctor accesses the PMR with or without patient's consent to provide timely treatment. The access during emergency can be

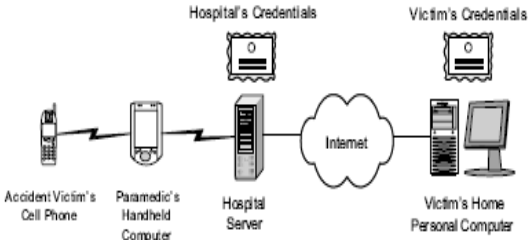

Fig. 1: Emergency Access to Patients' Medical

monitored and logged for future Accountability and Auditing (David *et. al.,* 2003).

The 4-Eyes Principle may be used where another authorized user (administer) with same or more privileges may access the system as observer in parallel to attending doctor to monitor the data access in emergency. Additionally, the data access activities can be stored in the users' smartcard/cell phone/PDA for the notification and future legal reparation. Only the primary physician may access the full medical record of the patient including history, whereas the secondary physician, the specialist or the attending doctor (in case of emergency) may access only partial record which is essentially required for the treatment at the particular time, disease or purpose. For example, if the patient is attended for eye-sore the doctor may not access (details of) any past surgery related to foot of the patient and the corresponding medical images or records related to any mental or emotional disorders of the patient.

4.3 CONTEXT AWARE ACCESS CONTROL

The *Context* in the Access Control Model may be used for dynamic authorization enforcement at the runtime using the constraints, as shown in **(Fig. 2)**. The context in broader terms may be anything like time, location, purpose or delegated rights etc. The contextual elements may be different for different roles in different scenarios and depend on other contextual elements. For example, a user with a role of specialist may access the patient's record only for the duration (time context) he is delegated rights for that within the physical boundaries of the hospital (location context), which my be verified by the specialist's PC IP address (Hu and Weaver, 2006).

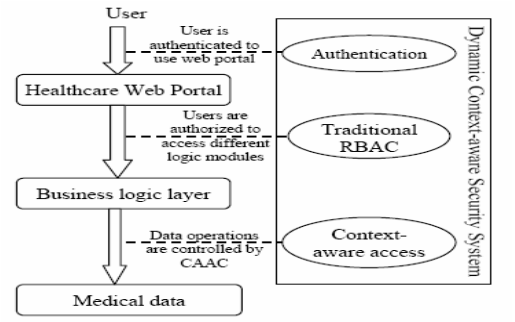

Fig. 2: Context-aware Access to Medical Records

4.4 PRIVACY PRESERVATION

The disclosure of data can be controlled and managed by the owner of data and should be based upon his privacy preferences and consent. The privacy of the patient's personal data in the eHealthcare System can be preserved by enforcing the privacy policy on data when the data leaves the owners' premises, as shown in **(Fig.3)**.

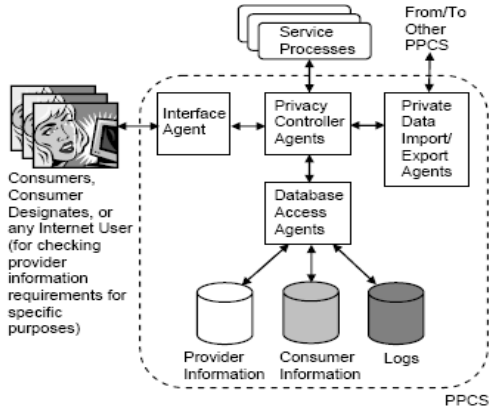

Fig. 3: Privacy Preservation for Medical Records

The user's privacy preferences are stored in the privacy controllers like smartcard, which verifies the privacy policies of requesting services checks their compatibility to the user's preferences, negotiates and then grants (or denies) access based on the negotiation decision. The users' privacy preferences, which are dynamic, can also be stored in the privacy profiles at the client component and the user can configure the client component and change the preferences anytime according to their requirements (Korba and Song. 2006).

The users and the services may disclose and negotiate their privacy policies before data transformation with or without the intermediate service (Trusted Authority), as shown in **(Fig. 4)**. The privacy policy comprises of the attributes of Collector (service), what data elements are requested, Purpose (use of data), Retention Time, Disclose-To (to other connecting or independent services). When data is requested by a service it should firstly be received by Privacy Preservation Module that checks the digital signatures of the requesting service and rewrites the data request query the Privacy Preferences of the data owner (Korba, 2005).

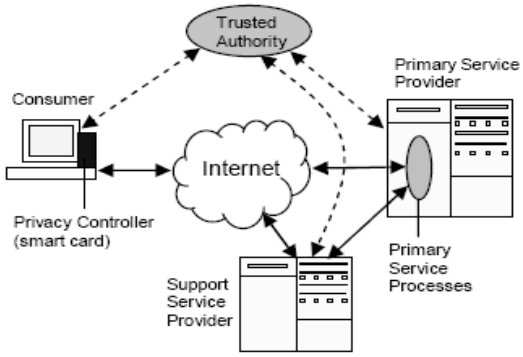

Fig. 4: Privacy Preferences of Data Owner

Alternatively the Privacy profiles of the users may be stored with the Trusted Authority that notifies and consents access to users' data by the services and monitors communication between owner of data and

collector service(s) of data, as shown in **(Fig. 5)**. The user data can be sent into the obfuscated packages with sticky policies which define disclosure constrains to sensitive data elements such constraints may be the policy attributes like Expiry-date, Purpose and Exposed-to information (Mont, *et. al.,* 2003). With the obfuscated data packages the information about the data owner's end also remains anonymous to the receiver of data.

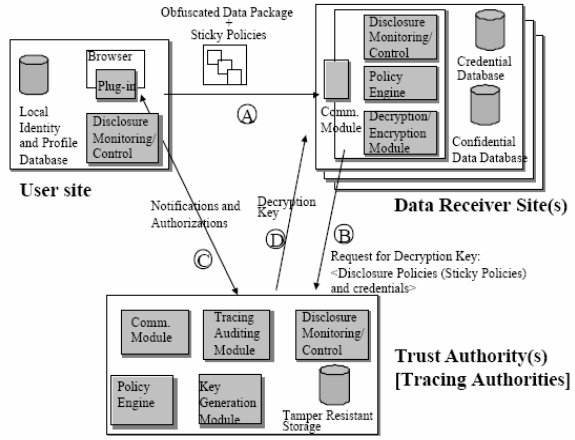

Fig. 5: Data Anonymization in Medical Systems

The eHealthcare system services collect all the user data for providing service to the consumer and that is threat to user's privacy as the user has no prior relationship or security domain compatibility with the services. For communicating to the services and disclosing private data to them some 'Trust Primitive' can be formulated with the service by disclosing a limited set of client attributes initially rather than sending all the attributes to the service and after the trust negotiation is accomplished on agreed upon contract, the user may sent further data to the services. This can be achieved by introducing an 'Attribute Service' at the client side that communicates with the data collecting service for trust negotiation (Wu and Weaver, 2005). The Trusted Intermediate Service may also verify if the platform of the data collecting services is 'Trusted', so that any uninformed dishonest use of the services can be prevented.

4.5 DATA ANONYMIZATION

The personal information of the user is not required when the data is used for the purpose of medical research in the vertical communication scenarios (disease management and research) therefore the data can be anonymized using Pseudonymization Service. In this process the PMR is divided into two parts the Personal Data and the Payload Data, as shown in Figure 6. The Personal data is assigned an algorithmatically generated code (Pseudonym) and the payload data is sent to the service with those Pseudonyms rather then sending the Personal Data to ensure Anonymity (DeMoor, *et. al.,* 2003). The algorithm used for the purpose should be verified so that it should disable any re-identification of the personal information from any data patterns.

4.6 ANONYMIZATION IN eHEALTHGRID SCENARIOS

Data Anonymization is also required to be performed by the middleware component in the eHealthGrid as shonwn in Figure 5. When patient's data is sent to health grid to share its shared computation service by the doctor/specialist for any further analysis which includes simulation and rendering. The pseudonyms are generated in this scenario for anonymization purpose in such a way that these are mapped back exactly to the original record of the patient (Fingberg, *et. al.,* 2006). Such simulation and rendering may also be required for the medical and industrial research purposes for the analysis of disease or the medicines or both.

5. CONCLUSIONS

Security and Privacy of medical data is huge challenge in current open systems processing data in the distributed service-oriented systems using vulnerable Internet network. Some of the architectures as discussed in this paper are capbale to meet these requirements. However, there are still many unslooved problems in the eHealthcare Security and Privacy domains:

a) When a physician accesses the medical records, he should not be able to further disseminate the user data to any other services that exploits the use of personal data for any business interests.

b) In the Mobile Privacy Preserving agents, used to enforce privacy at the remote services sites, it is difficult to secure those agents from the malicious code of the remote host and protect the remote host from the infected mobile agents. It is assumed that the Consent given by the data owner for the use of medical data is short-term, which expires within the lifetime of the data owner and the owner of data while giving consent doesn't know that what information may be useful in the future research, so this time-dependent short-term consents is not going to support the long-term research collaboration among the medical organizations.

Besides, Security and Privacy issues in the eHealthcare system need to be addressed keeping into view the legal rights for data protection and the systems should be so engineered to give the patient full control of data. The patient's consent should be ensured for use of their data assets and the services, which collect the user data should be accountable for access to the use of data to built user's confidence in the eHealthcare systems and services. The systems should be so designed so that the users don't need any special technical skills to use those systems.

System designing should be be abstracted from implementation for interoperability and productivity of software systems using the Model-driven Development

(MDD) approach and the systems should be service oriented to be easily extended and integrated to legacy new system. Finally the platform should be made more and more trusted to prevent tempering of the stored data.

REFRENCES:

Annas G. J. (2002) Medical Privacy and Medical Research: Judging the New Federal Regulations, The New England Journal of Medicine, **(346):** 216-220.

Blobel. B. and F. Roger-France (2001) A Systematic Approach for Analysis and Design of Secure Health Information Systems, International Journal of Medical Informatics, 62 **(1):** 51-78.

Chinaei A. H. and F. Tompa (2005) User-Managed Access Control for Health Care Systems, LNCS Journal, Vol. **(3674/2005):** 63-72.

David K., T. L. Sundelin, K. E. Seamons and C. D. Knutson (2003) Trust Negotiation for Authentication and Authorization in Healthcare Information Systems, Engineering in Medicine and Biology Society, Proceedings of the 25th Annual International Conference of the IEEE Los Alamitos Issue Vol. **(2):** 1406-1409.

David, C. P. (2010) Your Medical Records Aren't Secure. The Wall street Journal, March 23rd 2010.

De Moor, G.J.E., B. Claerhout and F. De Meyer (2003) PrivacyEnhancingTechniques-The secure communication and management of clinical and genomic data. Journal of Methods of Information in Medicine, 42 **(2):**148-53.

Dritsas, S. L. Gymnopoulos, M. Karyda, T. Balopoulos, S. Kokolakis, C. Lambrinoudakis and S. Katsikas (2006) A knowledge-based Approach to Security Requirements for e-Health Applications, Electronic J. Emerging Tools and Applications, Vol. **(2):** 01 Pp.

Emam K. E. (2006) Data Anonymization Practices in Clinical Research, A Descriptive Study, University of Ottawa, Canada.

Fingberg, J., M. Hansen, M. Hansen, H. Krasemann, L. L. Iacono, T. Probst, and J. Wright (2006) Integrating Data Custodians in eHealth Grids - A Digest of Security and Privacy Aspects, In GI Jahrestagung **(1):** 695–701.

Goldberg, D., E. Wagner, and E. Brewer (1997) Privacy-Enhancing Technologies for the Internet, IEEE COMPCON'97, 103-109.

Hu, J. and A.C. Weaver (2006) Dynamic, Context-Aware Access Control for Distributed Healthcare Applications, Department of Computer Science, University of Virginia.

Hung P. C. K. (2005) Towards a Privacy Access Control Model for e-Healthcare Services, In Third Annual Conference on Privacy, Security and Trust.

Kuenzi, J., P. Koster, and M. Petkovic (2009) Emergency Access to Protected Health Records. Studies in Health Technology and Informatics, **(150):** 705Pp.

Li, M. and R. Poovendran (2005) Enabling Distributed Addition of Secure Access to Patient's Records in A Tele-Referring Group. In: IEEE-EMBS (2005) Proceedings of the 27th IEEE EMBS Annual International Conference, IEEE, Los Alamitos. 308-317.

Lowrance W. (2003) Learning from Experience: Privacy and the Secondary Use of Data in Health Res., Journal of Health Services Research and Policy, Suppl. **(1):** S1:2-7.

Muhammad A., M. Hafner, R. Breu, and S. Unterthiner (2007) Framework for Modeling Restricted Delegation of Rights in SECTET. International Journal of Computer Systems Science and Engineering, 22 **(5):** 289-305.

Marco, C.M., S. Pearson and P.Bramhall (2003) Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services, Trusted Systems Laboratory, HP Laboratories Bristol.

Muhammad H., R. Breu, B. Agreiter, and A. Nowak (2006). SECTET: An Extensible Framework for the Realization of Secure Inter-organizational Workflows, Internet Research, 16 **(5):** 491-506.

Patrick C., K. Hung, J. Andrade, Y. Chen, R. Huang M. V. Martin and Y. Zheng (2007) Research Issues of Privacy Access Control Model for Mobile Ad Hoc Healthcare Applications with XACML, 21st International Conference on Advanced Information Networking and Applications Workshops, **(2):** 582-587.

Rannenberg, K., D. Royer, and A. Deuker (2009) The Future of Identity in the Information Society: Challenges and Opportunities, Springer Publishing Company Austria.

Win K. T. and J. A. Fulcher (2007) Consent Mechanisms for Electronic Health Record Systems: A Simple Yet Unresolved Issue, Journal of Medical Systems, 31 **(2):** 91-96.

Wu Z. and A. C. Weaver (2005) Dynamic Trust Establishment with Privacy Protection for Web Services", IEEE International Conference on Web Services (ICWS'05), Orlando, FL, USA.

Yee, G., L. Korba, and R. Song, (2006) Ensuring Privacy for E-Health Services, First International Conference on Availability, Reliability and Security - ARES' 06, Vienna, Austria.

Yee, G., and L. Korba, (2005) An Agent Architecture for E-Service Privacy Policy Compliance, 19th International Conference on Advanced Information Networking and Applications.