International Journal of Technology and Engineering System (IJTES)
Vol 6. No.3 – Jan-March 2014 Pp. 219-228
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

HEALTHFIT: FINE-GRAINED ACCESS CONTROL TO PORTABLE PERSONAL HEALTH RECORDS

M.Ramalingam
Research Scholar & Associate Professor
Dept. of Computer Science and Engineering,
Mailam Engineering College, Mailam – 604304, Tamil Nadu, India
rammalingamm2005@gmail.com

Dr.R.M.S. Parvathi
Principal & Professor, Dept. of Computer Science and Engineering
Sengunthar College of Engineering, Tiruchengode – 637 205, Tamilnadu, India

ABSTRACT

At present, rising potentialities for patients to access their health records or health info might probably cause changes among the present health supply system from Associate in Nursing institution-centered to a patient-centered model Associate in Nursing an electronic personal health record (PHR) might greatly influence such a shift. However, the employment of PHRs will introduce specific challenges in terms of accidental speech act of or malicious access to Associate in individual's health information. Hence a high level of security for information access is needed as a result of the sensitivity and confidentiality of the health information in PHRs. during this paper, we have a tendency to gift models for outlining and configuring fine-grained, role-based access management policies for XML-based moveable personal health records mistreatment Associate in extended digital certificate approach, referred to as Healthfit that permits versatile and dynamic communications while not employing a classical authorization and authentication approach like username and countersign.

Keywords: role-based access control; portable personal health record; XML document ;access control; health informatics

I. INTRODUCTION

Information and communication technologies have greatly pretentious the delivery of health care and can lead to aids in terms of quality and safety of patients. Health care providers have adopted electronic health care systems such as health information systems, clinical information system, and picture archiving and communication systems. Their adoption of such systems hypothetically improves record management such as the collection, integration and retrieval of patient's health records that have been typically stored in an electronic health records (EHRs) system, normally managed by an health care provider [23, 32]. Such institution-centered management of electronic health records can hypothetically deliver a barrier to patient's access to their health data for personal health activities such as decision-making and health planning [23].

Additionally, present emerging individual needs of patients to access health records or health information may hypothetically lead to vicissitudes within the current health care distribution system from an institution-centered to a patient-centered model and an electronic personal health record (PHR) may have an important role to play in such a shift[23]. Personal health records can be stored in various devices such as a standalone PC, portable storage devices including a smartcard[8],USB[35], a PDA or a mobile phone[28]or a web-based online server[23]. If personal health records are kept in personal portable devices, it may deliver individuals with greater control of their

health data [8, 23, 28] in terms of exchanging/sharing their health data with health care workers only when required. However, the use of PHRs or portable PHRs does introduce specific new challenges in terms of accidental disclosure of or hateful access to an individual's sensitive or confidential health data.

Due to such great sensitivity and confidentiality of the health data in PHRs and the fact that health data may need to be retrieved by a large number of health care workers with various roles for the care of the patient, the personal health record requires a high level of secure defense for data and data access. Approaches to securing the data access of the PHR could include role-based access control[15,18,32], attribute- based access control[10] or a declarative and secure access control model for health data based on XML representation[25]using various security implementations including key-based approaches [2,3,14,24].

To enforce reliable and trustworthy access control for precise management of personal health data accessed by many health care workers with different roles, this paper describes a declarative and secure access control model for portable personal health records (PPHRs), especially for the case of PPHRs stored in a mobile phone rather than other portable devices like USB, based on XML representation and an extended digital certificate, called Healthfit, providing a signed description of a particular health (mobile) entity and used for enabling secure communications between interacting parties[28].Our aim is to develop extensible models for defining and configuring fine-grained, role-based access control policies for XML-based movable personal health records using Healthfit which enables flexible and dynamic communications without using a classical authorization and authentication approach such as a username and password.

The remainder of the paper is organized as follows. Section II describes related work to this approach and Section III defines the architecture for the fine-grained role-based access control of portable personal health records based on XML representation and an extended digital certificate (i.e. Healthfit). Section IV describes how patients control their health data when they have communications with health care providers and a conclusion follows.

II. RELATED WORK

The emerging use of electronic personal health records by persons may hypothetically lead to frequent sharing and exchanges of required but access-controlled health information with health care workers through wired or wireless communications. Due to the sensitivity and privacy of health data, such activities require high security and stringent access control for a patient's health data to avoid malicious or accidental access to and possibly harmful use of the data. A classical authentication and authorization method such as the username and password approach could typically be used to build trusted communications between PHRs and systems (i.e. EHRs or a proprietary system) used by health care providers. The classical approach may need a module in the PHRs for administration and maintenance of lawful users such as a doctor by each individual owner of the PHRs and it may also give health care providers upsetting maintenance of a long list of username and passwords for his/her patients to access their PHRs. Otherwise, cryptographic technologies can be used for secure and trusted communications for authentication and data/information exchange and delivery of personal health records[14,24,32].

Healthfit[28] introduced an approach to role-based access to portable personal health records and its architecture may natively support a greater level of privacy using an protracted digital certificate-based approach. With a certificate called a Healthfit, the architecture can also provide establishment of flexible trusted communications between parties previously unknown to each other (health care providers and patients)under an unpredictable and dynamic mobile computing environment. The Healthfit architecture builds from the MobiPass architecture[29] here applied to the PPHR domain. With the possible future usage of such body area network (BAN)-based technologies as health devices [26,27] a PPHR architecture may be easily integratable and also particularly helpful of patient privacy.

Additionally,the Healthfit architecture provides two flexible communication modes in terms of sensitivity level of data/information involved in communications: wireless communication or communication based on physical docking. The wireless communication mode is used for unsecure data exchange or sharing such as for pharmacist product advertising to a patient and the physical-docking communication mode is used for secure and private data exchange such as for accessing personal health data during a consultation. However, Healthfit in [28] does not discuss 1) granularity of secure access control to personal health records such as a part of a record (e.g. medical history) and 2) stored data representations such as relational database or XML-based representation. In this paper, an XML representation is considered for the PHR data structures due to the widespread use of XML for

hierarchical semi-structured representation of documents and its standardization for data storage and exchange[33]. Much work for secure access control for XML documents has been studied due to such reasons.

Xplore [25] described a flexible and declarative access control model for XML documents including XML-based electronic health records and utilized fine-grained access control policies that define declarative access control rules and privileges based on different access roles. As a personal health record is composed of fragments of information with various sensitivity levels, Xplore can provide reliable control of sections of the XML document (health record) in terms of defined rules enforced by semantically hierarchical access privileges associated with defined access roles and security levels of users. Xplore may provide greater control of secure accessibility to XML-based data in the health domain. However, Xplore requires an expensive computing cost to scan each element for access decisions when user access occurs. Unlike defined roles in a single domain as in Xplore, privacy-aware role-based access control [18] described dynamic and flexible role provisioning by mapping roles of users in multi- domains to those of an organization controlled by its own security and privacy policies under a pervasive eHealth environment.

Much other work has focused on secure views of XML documents based on access control specifications and/or rules applicable to DTDs (Document Type Definitions)/schema, instance, element or attribute-value levels. eXtensible Access Control Markup Language (XACML) [22] standardizes an access request/response format, architecture of the policy enforcement framework, etc. Gabillon and Bruno[11] addressed secure access control (i.e. read privilege) for XML documents based on XPath and XSLT(eXtensible Stylesheet Language Transformations) languages that interpret authorization specifications rules supporting protection granularity of data at the levels of node and content in XML document structures.

Stoica and Farkas [30] generated partial secure views based on modification of DTDs in terms of assigned access permissions to XML documents and tags by plummeting semantic conflicts of associated tags in the DTD. But it did not cover data-level protection of XML documents. Security Views [9] discussed a DTD-based access control model enforced by security constraints (access specifications) and XML query evaluation enabled by XML query rewriting and an optimization algorithm. Goel et al. [13] discussed building access control specifications (rules) from data and/or predefined access rules by using XQuery.

Generalization of XML security views [16] applied to access control (authorization) specifications to DTDs for DTD annotation is fully extended to annotated XML documents for secure views by annotating and building view algorithms such as node pruning. IPAC (Interactive approach to Access Control for semi-structured data) [20] describes a framework for XML access constraint specification and manual selection of security views ranked by several parameters to assist database administrators in specifying optimal access control strategies. Unlike IPAC, mapping declarative access control constraint specifications to a defined security specification language for XML was used to generate possible candidate security views by view ranking parameters such as potential information leakage[33].

Damiani et al. [5, 7] discussed secure access control of repositories of XML documents for secure views. The access to XML documents was controlled by access authorization specifications and two processes such as labeling and pruning. XUpdate language [6] focused on a secure updating mechanism for XML documents and the mechanism was based on rewriting procedures of XML schema, using deterministic finite state automaton, that was annotated with authorization attributes. Abiteboul et.al. [1] addressed secure access control of health records employing a peer-to-peer architecture that can handle distribution of data and integrated AXML(Active XML)document management framework with secure management of distributed XML data. Wang and Osborn [34] applied role-based access control for XML documents using graphic models (e.g. role graph model) and defined hierarchical roles and privileges belonging to each role that were inherited to its senior role (parent role) in the hierarchy.

Research work mentioned above focuses on generation of secure views or updates of XML documents for authorized users in terms of declarative access control specifications and policies but secure data exchange and transmission via networks is also an important issue for protection of sensitive health records from malicious and unauthorized interception. Cryptographic technologies have been used for both access control for secure views and encrypted data transmission to authorized users.

Author-X [2] discussed encryption-based secure access control (browsing and authoring) and its administration defined by a declarative policy for XML documents. Bertino and Ferrari [3] also

discussed secure delivery of XML documents in terms of encryption of portions of the same document with their associated encryption keys which are selectively dispersed to various users according to defined access control policies. Secure data publishing based on a symmetric cryptographic technology for XML-based documents employed declarative policy queries and rewriting rules for optimization and normalization of secured XML-trees for guard [19]. Unlike other approaches mentioned previously, an approach that discussed access control on encrypted XML data at the client side rather than at the sever side, especially lightweight devices under secure operating environment is found in [4]. Garson and Adams [12] addressed policy-based encryption technology for access control in a health care environment.

Our work extends ideas deliberated in access control research focused on the declarative access policy (rules) for XML documents such as health records [25] and flexible and dynamic trustworthy communications for authentication and authorization by using an extended digital certificate [28].

The portable personal health record (PPHR) as a kind of PHR could doubtless contribute to up the access to and management of a patient's health knowledge. For example, a patient's info like his medical take a look at results and medications may be wont to improve clinical decision-making at the purpose of care even if the unit several technical problems to deal with. Owing to the sensitivity and privacy of such personal health knowledge, sharing and exchanges of a patient's health info with a health care employee needs technically sure and secure communications.

The Healthfit design [28] will produce sure physical arrival or sure wireless communication underneath a dynamic and unpredictable mobile computing surroundings within the health domain and provides larger flexibility than a certificate authority. Additionally, the PPHR design supported Healthfit and XML illustration, that is made closely from the MobiPass design [29], ought to offer fine-grained roughness of protection for all or a part of a patient's health knowledge in a very moveable mobile device. Hence this design can build(1) secure associated trustworthy communications between unknown health entities victimization an extended digital certificate instead of classical authorization and authentication approach (Fig.1 and 2) secure protection of the health record through a role-based access management policy for the certified health entities requesting access permission for half or all of the private health record hold on within the mobile device (Fig.2). underneath this design, a patient because the owner of the PPHR will outline the role-based access management policy for the health knowledge within the PPHR and manage his/her health records firmly and in private underneath the patient's own management. Fig.1 shows the design of a PPHR employing a mobile device (e.g. a personal organizer or a mobile phone) for private health records.

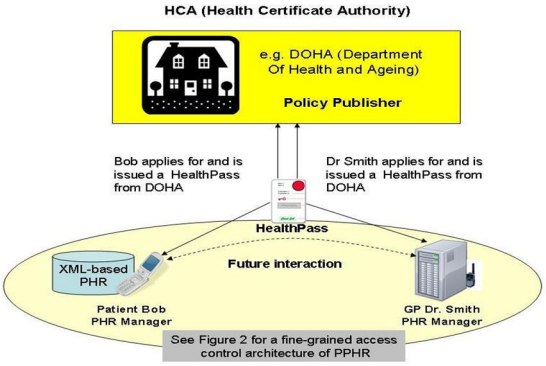


Figure 1.Overall portable personal health record (PPHR) architecture with XML-based PHR – PHR certificate (Healthfit) issuing

The approach assumes that all health care providers and patients should be registered with an authority such as a Health Department (Department of Health and Ageing in Australia) and such a body would equate with a HCA (Health Certificate Authority) in this architecture. The architecture is calm of four major components: HE (Health Entity) policy, Healthfit, HCA (Health Certificate Authority), and PHR Manager (Personal Health Record Manager). We will briefly describe each component in the PPHR architecture seen in Fig.1.

HE (Health Entity) Policy describes attributes of health (mobile) entities such as a globally unique ID issued by a HCA for example DOHA, health care provider unique identifier number and attributes with other policy-related information. HE policy illustration follows an XML schema format to allow extensible description of services and dynamic evaluation of mobile entities.

Healthfit is a digitally signed description of a particular health entity, which is issued by a HCA and enables trusted and flexible communication in a dynamic mobile environment. A Healthfit representation is as an XML instance document (e.g. attribute and value pair) (see [28] for further detail).

HCA (Health Certificate Authority) (e.g. could be DOHA
– Department of Health and Ageing - in Australia in the health domain) issues digital certificates (Healthfit) to entities in the health system – these would be individuals, providers or potentially other entities. The HCA evaluates such entities based on the HE

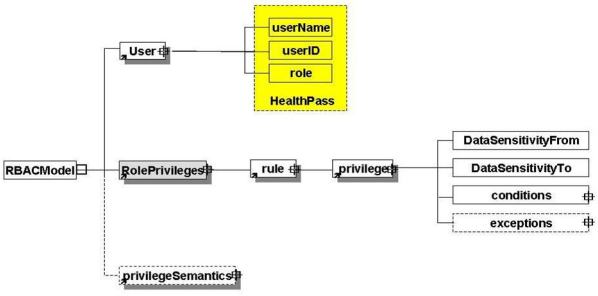
Policy and produces a digital signed result of the evaluation (e.g. Healthfit). Under the Healthfit architecture, the Healthfit might typically only be issued to a health (mobile) entity by the HCA through an offline application and authentication process. In addition the HCA can also optionally play a policy publisher role.

PHR Manager (Personal Health Record Manager) is software package resident on the mobile device of AN entity and is invoked if and solely if devices square measure physically connected along for secure health communication show ever is wirelessly for different during this paper, the PHR Manager's practicality to make sure communications between to antecedently unknown to every different mobile (health) entities won't be mentioned(see details in [28]) however we have a tendency to can focus on PHR Manager's actions for application of a fine-grained access management policy, outlined by the owner of the PPHR, that enables licensed users like a MD, a dentist, or a druggist to access jus the required and licensed fragments of private health records within the PPHR. The licensed users valid and verified by their Healthfit by the PHR Manager will then access the PPHR with their allowable access privileges like scan and browse and/or write. as an example, an outlined access management rule might be that a GP will see all of the patient's health records as well as personal detail, medication, and designation, etc. or a druggist will exclusively see medication records associated with a particular health condition. To do this, the PHR Manager interconnects with AN access management social control module(Fig. 2)within the PPHR by transmitting collected information from an incoming Healthfit like Healthfit ID, a task like doctor or a druggist and name etc. At now, role allocation for the user of the incoming Healthfit is done either manually or mechanically. If the incoming Healthfit first interacts with the PPHR, then the PHR Manager will invoke manual setting for a task and its associated access management rules for the Healthfit in terms of the outlined access management policy. The owner of the PPHR will outline or dynamically update roles and their associated access management rules through a security administration module once needed.

Alternatively, the PHR Manager will mechanically assign and set a task and its associated access management rules for the incoming Healthfit once

1)the Healthfit isn't unaccustomed the patient's PHR Manager because it had its previous preference setting for a task and access management rules appointed to the Healthfit that was already hold on within the patient's Healthfit repository and

2)the access management module applies the patient's access control policy to the incoming Healthfit directly, while manual favorite setting to the new Healthfit, by exploitation the contents of the Healthfit that maybe understood and picked up by the PHR Manager like world individuality and its job class. as an example, if the incoming Healthfit belongs to a doctor, then the PHR Manager understands the contents of the valid and verified Healthfit and informs the access management social control module of the task class, as doctor. Then the access management module can mechanically assign a task (doctor) and its associated access management rules to the Healthfit in terms of the patient's access control policy. By such seamless communications with the PHR Manager, the access management social control module can generate licensed health info supported access privileges outlined for the known role of the incoming Healthfit's owner and come the licensed health information to the PHR Manager to send them to the health entity of the incoming Healthfit. At this step, the PHR Manager happiness to a health care supplier can move with a general application to show licensed data transmitted from a patient's PPHR. Some major problems in electronic personal health record square measure tight access management, security of patient information and protection of privacy of a patient. The projected PPHR design supported the Healthfit design provides patient-driven access management for licensed users and protection of privacy of a patient's health information. Now, we'll specialize in the fine-grained access management framework for PPHRs primarily based on XML illustration, XML being in wide use and standardization for information storage and exchange.



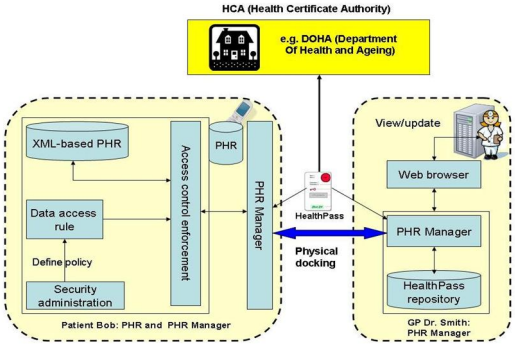


Figure 2. XML-based PPHR enabling fine-grained role-based access control

The detailed architecture of the XML-based PPHR enabling fine-grained role-based access control is shown in Fig.2. The PPHR system will rely on XML schemas of the health data as well as access control rules distinct by the PPHR access control policy and encoded using the proposed constraints used in XML. The access control implementation module will enforce access control rules defined for roles of authorized users which the PHR Manager can verify with their Healthfit. In this paper we will focus on the XML security features of the framework and clear and simple declarative specification picture to encode the semantics of the access control policy rather than applying access control rules to XML documents to effectively and efficiently generate secure views (or apply secure update) for XML documents like well-known methods such as rewriting

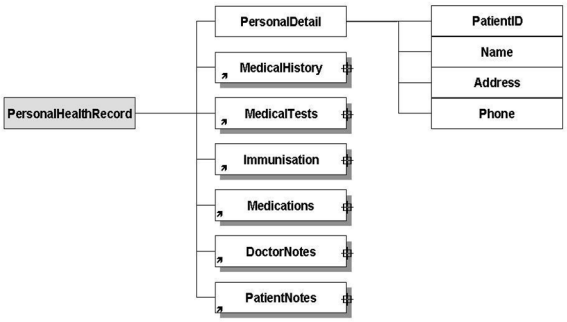


Figure 3. Hierarchical privileges

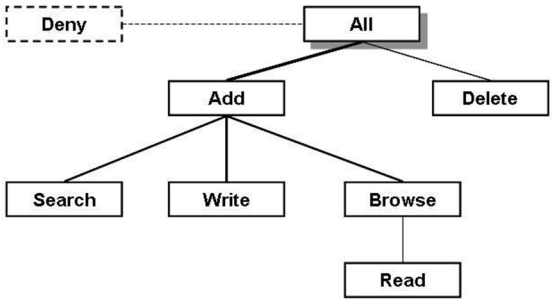


Figure 4. PPHR data model

The role-based access control model is shown in Fig. 3 and the set of possible hierarchical privileges (Fig. 4) would be read, write and other privileges (see detailed meanings of rights and their semantic relationships in [25]) . Unlike the Xplore architecture [25], this model uses Healthfit information, composed from a verified Healthfit such as an authorized user's information and role, to allow the role to be attached to the authorized user. Amongst other things, it allows granularity of protection levels of data by adding a sensitivity attribute/value to elements of an XML data schema.

We assume an example of XML-based PPHR data illustrate the concept of the proposed approach. You can also refer to detailed data types for personal health records from the Markle Foundation[17]. Suppose that a patient wants to impose the following security policy on his/her personal health record, with two simple types of roles defined in the security policy, namely Doctor and Patient, according to the following access control:

1. The authorized doctor can access a patient's PHR allowed by the doctor's role. For PatientNote, the doctor can only read but not add or update.

2. A patient is allowed to access all his/her personal health record. For DoctorNote, the patient can only read but not add or update.

An access control policy consists of a set of declarative rules (the „data access rule' component in Fig. 2) and describes privileges of user roles that restrict access to sections of the XML document with various compassion levels (Fig. 6). The access control implementation module, which interacts with PHR Manager, will apply the access control policy based on the role that is assigned to the authenticated and authorized user by the access control policy for the above constraints can be effortlessly defined as it is based on the role of the user and its admittance privileges allowed for the distinct role type by

adding the data compassion level into the existing data model schema. The data compassion levels would depend on the access control policy defined by the owner of the PPHR yet we have decided four sensitivity levels, represented by the integer value of 1 to 4, where Level 1 denotes elements that are unclassified to Level 4 that represents elements that are consider highly classified. For the above example 2, DoctorNote can be highly sensitive data rated as sensitivity level 4. Fig. 7 shows an example of a PPHR XML schema representation for DoctorNotes element and Fig. 6 shows an example of access policy encoded via declarative access control rules for the Doctor role.

In this section, we have discussed a fine-grained, role-based access control architecture utilizing an extended digital certificate, Healthfit, for flexible authentication and authorization. The architecture also defined an access control model containing of declarative access control rules defined by data sensitivity level, role and privilege. In the next section, we will explain example scenarios of the working of fine-grained access control to PPHRs based on an protracted digital certificate, Healthfit architecture.

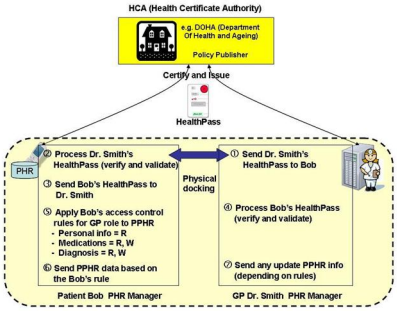


Figure 5. Example of PPHR XML schema

IV.FINE-GRAINED ACCESS CONTROL TO PORTABLE PHRS

The Healthfit architecture creates dynamic and flexible communication between previously unknown to each other health (mobile) entities in an unpredictable wireless or physically docked environment. Due to the sensitive and private nature of health data in PPHRs, two modes of communication are proposed: PHR Manager invokes personal health record access mode when two health (mobile) entities are physically linked together and PHR Manager invokes a wireless mode when the patient'smobile entity recognizes a wirelessly incoming Healthfit which is not related to personal health record access or outflow of information e.g. a pharmacy sends new medicine information to registered customers. We will describe the example application of the fine-grained role-base access control of PPHRs between a patient and 1) a GP and 2) a pharmacist.

A. Example 1. Bob sees his GP Dr. Smith:

Bob is a patient and Dr. Smith is a general practitioner. We assume Bob physically links his mobile phone stored with his PPHR to Dr. Smith's device that can enable PHR Managers to interact in the PPHR architecture in Dr. Smith's office. Both health (mobile) entities will exchange their Healthfit to verify and validate each other. If Dr. Smith's Healthfit is verified and validated, then Bob's PHR Manager interacts with the access control enforcement module in his PPHR (see Fig. 2) to allow access privileges according to the role allocated to Dr. Smith. For example, if Dr. Smith is allocated a 'Doctor' role by Bob, then he can access Bob's health data with sensitivity levels from 1 to 4 in terms of Bob's access control policy (Fig. 6). Default sensitivity levels of DoctorNotes and Medication elements are 4 and 2. With these access control rules and constraints, Dr Smith can have authorized access privileges to all health data in Bob's PPHR except for exceptional conditions in Fig. 6. For example, Dr Smith is allowed to search and browse Bob's PatientNotes element.

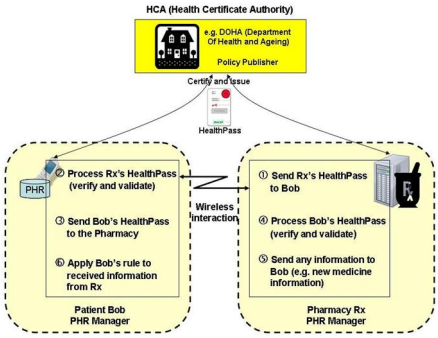


Figure 6. Personal health record communication between a patient and a doctor (a general practitioner).

If the access control enforcement module in the PPHR returns health data authorized for Dr. Smith to his PHR Manager, then Bob's PHR Manager transmits the data to Dr. Smith's PHR Manager which will interact with a standard web browser to show Bob's health data to Dr. Smith (step 5 and 6 in Fig. 8). Dr. Smith can also add, for example, DoctorNote to or update Bob's PPHR if Bob's access control rules defined for Dr. Smith allow any add or update privileges to his PPHR. In this paper, the application technologies of access control rules for viewing and updating XML documents such as filtering, rewriting, pruning, and labeling methods will not be discussed in detail. In addition, the access and deal logs for auditing a PPHR system will not be also discussed in detail in this paper.

B. Example 2. Bob receives information from a pharmacist:

A PHR Manager can invoke a wireless trusted communication mode when there is an incoming Healthfit from a pharmacist that registered with a HCA to obtain the Healthfit. The pharmacist may send any medication information through a wireless network to Bob's mobile phone. At this time, Bob can receive the inflowing information from the pharmacist without giving any access privilege to his personal health record. Non-physical docking to a PPHR-enabled device does not allow any access to Bob's personal health records for information outflow, hence ensuring PPHR security.

However, if Bob wants to interact with the pharmacist to purchase any medicine with electronic prescription stored in his PPHR that was prescribed by his family doctor, then Bob needs to physically link his mobile phone with PPHR-enabled device in the pharmacist to interact together. The PPHR access process would be the same as in the Example 1 above. Examples shown during this section describe to modes of the patient management of their personal health records in transportable mobile devices and fine-grained role-based access management of their personal health records by victimization info collected from verified Healthfit. The access management model consists of declarative access management rules outlined by knowledge sensitivity level, role and privilege. With the sensitivity level declaration at the schema level, a native declaration on any sub level part will be accustomed override the cascaded sensitivity level. Otherwise the outlined sensitivity level would propagate all the way down to the sub-elements.

V.CONCLUSION

We have planned a fine-grained, role-based access management design for PPHRs to supply a patient with higher management and protection of their personal health records. This design is based mostly on the trustworthy communication design employing a signed extended digital certificate (Healthfit) issued by a certificate authority (HCA e.g. may be El Beda in Australia) and a XML-based declarative access management model, consisting of a set of privileges and access management rule schemas, which offer powerful quality to inscribe access rules for semi-structured content. we tend to conjointly in contestible the mixing of this trustworthy communication design with the access management framework – the access management module during a PPHR interprets access control rules and applies outlined privileges of users to XML-based personal health records. This design conjointly supports to modes of versatile communication between mobile entities: trustworthy communications between physically coupled entities for secure access management of knowledge outflow and trustworthy communications between unknown mobile entities below an unplanned and dynamic wireless surroundings. Our future work can study access management to XML repositories victimization XML views [21] and users appointed to multiple roles and the roles' hierarchic relationships related to access privileges for the roles below distributed XML repositories.

REFERENCES

[1] S. Abiteboul, B. Alexe, O. Benjelloun, B. Cautis, I. Fundulaki, T. Milo, A. Sahuguet, "An electronic patient record "on steroids": distributed, peer-to-peer, secure and privacy-conscious", VLDB 2004, Canada, pp. 1273-1276, 2004.

[2] E. Bertino, S. Castano and E. Ferrari, "Securing XML documents with Author-X", Internet Computing, IEEE, vol. 5, pp.21–31, 2001.

[3] E. Bertino and E. Ferrari, "Secure and selective dissemination of XML documents", ACM

Transactions on Information and System Security (TISSEC), vol. 5, pp. 290–331, 2002.
[4] L. Bouganim, F.D. Ngoc, P. Pucheral, "Dynamic access-control policies on XML encrypted data", ACM Transactions on Information and System Security (TISSEC), vol. 10, pp. 1-37, 2008.
[5] E. Damiani, S. de Capitani di Vimercati, S. Paraboschi and P. Samarati, "A fine-grained access control system for XML documents", ACM Transactions on Information and System Security (TISSEC), vol. 5, pp.169–202, 2002.
[6] E. Damiani, M. Fansi, A. Gabillon and S. Marrara, "Securely updating XML", KES 2007, Italy, pp. 1098-1106, 2007.
[7] E. Damiani, P. Samarati, S. de Capitani di Vimercati and S. Paraboschi, "Controlling access to XML documents', Internet Computing, IEEE, vol. 5, pp.18–28, 2001.
[8] S. Endsley, D.C. Kibbe, A. Linares, and K. Colorafi, "An introduction to personal health records," Family Practice Management, pp. 57-62, May 2006.
[9] W. Fan, C. Chan, and M. Garofalakis, "Secure XML querying with security views", ACM SIGMOD International Conference on Management of Data (SIGMOD '04), France, pp. 587-598, 2004.
[10] K. Frikken, M. Atallah, and J. Li, "Attribute-based access control with hidden policies and hidden credentials," IEEE Transactions on Computers, vol. 55, pp. 1259-1270, 2006.
[11] A. Gabillon and E. Bruno, "Regulating access to XML documents", Annual Working Conference on Database and Application Security (Das'01), Canada, pp. 299-314, 2001.
[12] K. Garson and C. Adams, "Security and privacy system architecture for an e-hospital environment," Symposium on Identity and Trust on the Internet, USA, pp. 122-130, 2008.
[13] S.K. Goel, C. Clifton and A. Rosenthal, A. (2003) "Derived access control specification for XML", ACM Workshop on XML Security, USA, pp. 1-14, 2003.
[14] G. Kambourakis, I. Maglogiannis, and A. Rouskas, "PKI-based secure mobile access to electronic health services and data," Technology and Health Care, vol. 13, pp. 511-526, 2005.
[15] D. Kulkarni and A. Tripathi, "Context-aware role-based access control in pervasive computing systems," ACM symposium on Access control models and technologies, Estes Park, USA, pp. 113-122, 2008.
[16] G.M. Kuper, F. Massacci and N. Rassadko, "Generalized XML security views", Int. J. Inf. Sec. (IJISEC), vol. 8, pp. 173-203, 2009.
[17] Markle Foundation, "Connecting for health a public-private collaborative", 2003, available at: http://www.connectingforhealth.org/resources/final_phwg_report1.pdf
[18] L.D. Martino, Q. Ni, D. Lin,and E. Bertino, "Multi-domain and privacy- aware role based access control in eHealth", International Conference on Pervasive Computing Technologies for Healthcare (Pervasive Health 2008), Finland, pp. 131-134, 2008.
[19] G. Miklau and D. Suciu, "Controlling access to published data using cryptography", VLDB 2003, Germany, pp. 898-909, 2003.
[20] S. Mohan and Y. Wu, IPAC - An Interactive Approach to Access Control for semi-structured data, VLDB 2006, Korea, pp. 1147-1150, 2006.
[21] V. Nassis, R. Rajugan, T.S. Dillon, and W. Rahayu, "Conceptual design of XML document warehouses", International Conference on Data Warehousing and Knowledge Discovery (DaWaK 2004), Spain, pp. 1- 14, 2004.
[22] OASIS, "eXtensible Access Control Markup Language (XACML) Version 1.0", available at: http://www.oasis-open.org/committees/download.php/2406/oasis-xacml-1.0.pdf, 2003.
[23] J.B. Perlin, R.M. Kolodner and R.H. Rosswell, "The veterans health administration: quality value, accountability, and information as transforming strategies for patient-centered care", Am J Manag Care, vol. 10, pp. 828-836, 2004.
[24] U. Sax, I. Kohane and K.D. Mandl, "Wireless technology infrastructures for authentication of patients: PKI that rings," Journal of American Medical Informatics Assoc, vol. 12, pp. 263-268, 2005.
[25] R. Steele, W. Gardner, D. Chandra, and T.S. Dillon, "Framework and prototype for a secure XML-based electronic health records system," International Journal of Electronic Healthcare, vol. 3 pp. 151-174, 2007.
[27] R. Steele, A. Lo, "Future Personal Health Records as a Foundation for Computational Health". Computational Science and Its Applications -ICCSA 2009, Lecture Notes in Computer Science, Volume 5593/ 2009: 719-733.
[28] R. Steele and K. Min, "Role-based access to portable personal health records", International Conference on Management and Service Science (MASS (EMS/ISM) 2009), Beijing, China, 2009.
[29] R. Steele and W. Tao, "MobiPass: A passport for mobile business," Personal and Ubiquitous Computing, vol. 11, pp. 157-169, 2007.
[30] A. Stoica and C. Farkas, "Secure XML views", IFIP WG 1.3 International Conference on Data and Applications Security, UK, pp. 133-146, 2002.
[31] A. Tripathi and M.M. Gore, "Hasslefree: Simplified access control management for XML document", International Conference on

Distributed Computing and Internet Technology (ICDCIT 2007), India, pp. 116-128, 2007.
[32] F.K. Uckert and H. Prokoschl, "Implementing security and access control mechanisms for an electronic healthcare record," AMIA Symp, pp. 825–829, 2002.
[33] W3C-XML, Extensible Markup Language (XML), http://www.w3.org/XML, 2004 [34] J. Wang and S.L. Osborn, "A role-based approach to access control for XML databases", SACMAT 2004, USA, pp. 70-77, 2004.
[35] A. Wright and D.F. Sittig, "Encryption characteristics of two USB-based personal health record devices," Journal of American Medical Informatics Assoc, vol. 14, pp. 397-399, 2007.