A Secure Real Media Contents Management Model Based on Archetypes using Cloud Computing

You-Jin Song[1], Jang-Mook Kang[2] and Jaedoo Huh[3]

[1]*Department of Information Management, Dongguk University,*
707 Seokjang-dong, Gyeongju, Gyeongsangbuk-do, 780-714, Korea

[2]*Electronic Commerce Research Institute, Dongguk University,*
707 Seokjang-dong, Gyeongju, Gyeongsangbuk-do, 780-714, Korea

[3]*Real&Emotion Sense Convergence Service Research Section*
Smart Green Life Research Department
IT Convergence Technology Research Laboratory
Electronics and Telecommunications Research Instutite(ETRI)
song@dongguk.ac.kr, jdhuh@etri.re.kr

Abstract

This paper presents modifications and improvements to the interface of a secure real media contents management model with the intention of increasing security and usability. This paper examines a security technology that needs to be considered in the EHR (Electronic Health Record) service model. This EHR(Electronic Health Record) service model is suitable for example a secure real media contents management & processing. It constructs a model based on a MVC (Model-View-Controller) pattern based on access rights and distributed management. In particular, it constructs a test bed utilizing the Open EHR Tool which is a major topic in this area. Through this, it suggests the EHR service security control model in the context of the patient and medical team. Our work aims for a new way of structuring, storing and managing patient data so that they can be shared and exchanged between different healthcare providers and other stakeholders in a safe and secure manner.

Keywords: *Medical sensing information, EHR (Electronic Health Record), Security management, context-awareness, MVC Pattern*

1. Introduction

In the era of the smart-phone, this device can be utilized as a mobile medical support device containing diverse sensors. The smart-phone certainly serves as a type of USN (Ubiquitous Sensor Network) through implanted chips and sensors in the living area, as well as in the human body gathering medical information. In order to realize a healthcare service, a digital network of medical information should be prepared. For a personalized medical service, a context-aware system using sensing needs to be implemented.

A context-aware based medical service model can be developed by referring to the EHR (Electronic Health Record) model. Using the EHR model, doctors and nurses can share the patients' medical information. However, networked health information has hazards of intentional leaking of personal information. It also may face the risk of trading, unauthorized viewing or copying of medical information.

This paper deals with using the specific health information of context-awareness and security. In particular, it views security needs that should be considered in the EHR service model and constructs models based on the MVC pattern about access rights and distributed management. It also studies the application of the security management of web based EHR services through the construction of a test-bed utilizing the OpenEHR Tool, the major topic in this area, and examines the solution. Our involvement led to the emergence of OpenEHR as a new way of structuring, storing and managing patient data so that it can be shared and exchanged between different healthcare providers and other stakeholders in a safe and secure manner [1].

2. Relevant Studies

2.1 OpenEHR

Ocean Informatics is an Australian health informatics company developing a comprehensive tool set for the construction of open interoperable systems for shared electronic health records. Ocean Informatics has partnered with University College London to establish the OpenEHR Foundation– a non-profit registered charity – to promote and support the open Electronic Health Record initiative, known as OpenEHR [1]. OpenEHR aims for the description of a personal requirements specification about the general requirements that are necessary to express and communicate EHR information. The requirements are divided into the solutions about the EHR information architecture, the model, and the terms. Also, it provides a reference base that an EHR system developer can validate during the EHR system construction process. Such a series of processes is done by cooperation with other sectors in the medical information area [2].

The EHR architecture is an information system that consists of components about health records. And HER communication based on archetype methodology has been developed by openEHR and CEN/ISO[17]. According to ISO 18308:2011(Health informatics-requirements for an electronic health record architecture), the EHR architecture is defined as "The generic structural components from which all EHRs are built, defined in terms of an information model"[3].

The EHR architecture should be expressed, depending on viewpoint, as a 4-level model consisting of a context model, a concept model, a logical model, and a physical model. It is also divided into business architecture, data architecture, application architecture and technical architecture, depending on the modeling objects of the EHR system. The international standardization organizations relating to the EHR architecture are the ISO, CEN, HL7, OpenEHR, *etc.* [4]

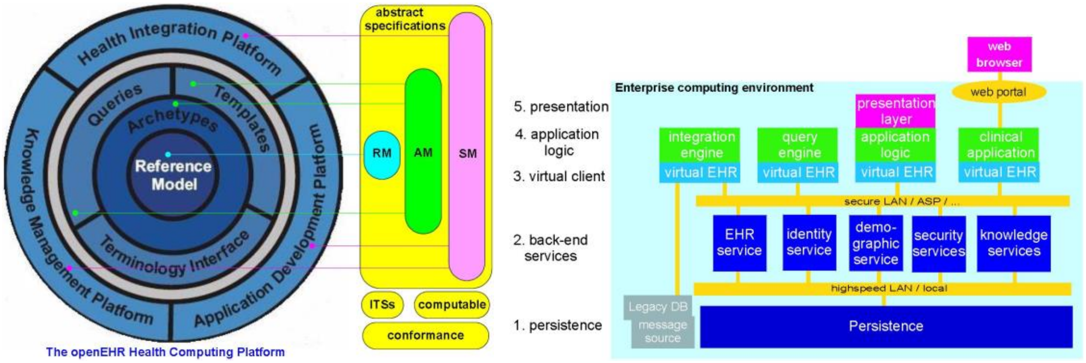

Figure 1. openEHR Health computing Platform and System Architecture [15]

The EHR system model that OpenEHR proposes consists of a 5-tier system architecture. The detailed technology specifications are as follows.

- Persistence: This is the stage which conducts the saving and searching of the information.

- Back-end Services: This includes EHRs, vital statistics, technical terms, structure, and location of security records.

- Virtual Client: This is the middleware that consists of a logical set of APIs. There are related services that can access various back-end services.

- Application Logic: This describes in detail applications that include various types of logic. For example, a user application such as the query engine operates in Application Logic.

- Presentation: This is the application layer that consists of the graphic interface.

OpenEHR provides tools as follows. The tools below help in the integration of the information architecture, model, and terms.

The Clinical Knowledge Manager acts as a web portal which provides various Archetype models and shares them. In particular, web developers will download desirable Archetype models and construct web applications. Recently, 200 useful Archetype models that satisfy ISO13606 were provided [5, 6]. The Clinical Knowledge Manager provides OpenEHR Archetype's GUI in the form of a mind map. It also shows Archetype's definition [Figure 2, Figure 3].

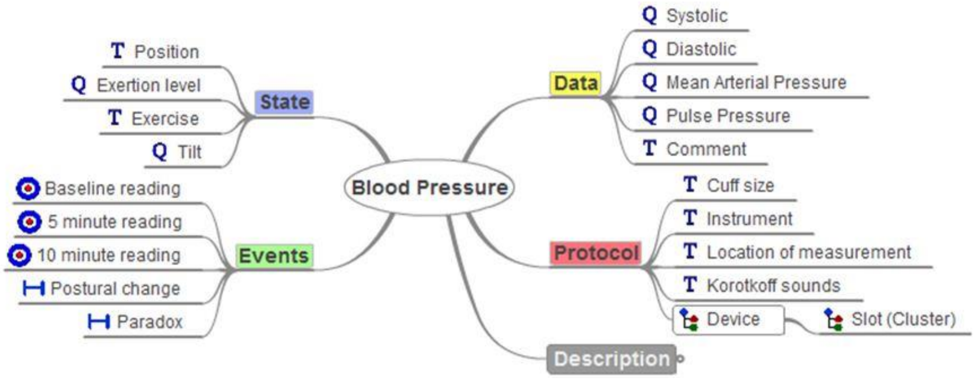

Figure 2. Mind map of sample blood pressure information.v1 [16]

Figure 2 shows a case of implied blood pressure information with the mindmap image of archetype. It is also a mind-map about blood pressure information collected by using the Clinical Knowledge Manager. This mind-map can draw from the EHR (Electronic Health Record) model that is open for common use in the hospital. For this, the blood pressure information is mapped by state, events, data, protocol and description. This categorized mind-map is a group about blood pressure information based upon ISO13606.

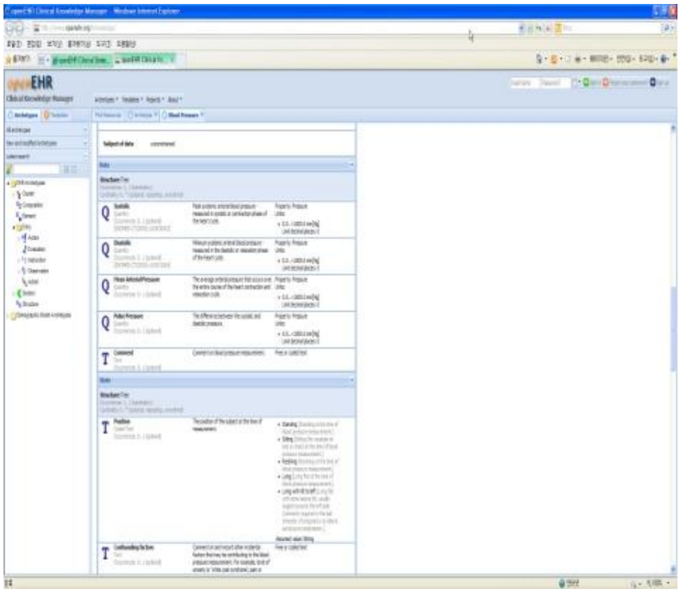

Figure 3. Definition of sample blood pressure information v.1 [18]

Figure 3 is a definition about the detailed function of the mind map as shown in Figure 2. With regard to blood pressure's function, definition and service, we can rapidly draw an archetype model through the same method as described in both Figure 2 and Figure 3.

The Archetype model provided by Clinical Knowledge Manager can be printed out as an XML form through the Archetype Editor. The Archetype Editor developed by Ocean Informatics is an editing tool redefining the Archetype model.

The web-based EHR developers redefine Archetype models provided by Clinical Knowledge Manager. An Archetype model that has been modified into a desirable structure can be printed out in an XML form that fits to the OpenEHR Architecture model [7].

2.2 MVC Pattern

The MVC(Model-View-Controller) pattern provides the application's visual elements by separating the business logic from the user interface. Also, it can produce an application that can easily modify the business logic that is run in the background without the components affecting each other [Figure 4].

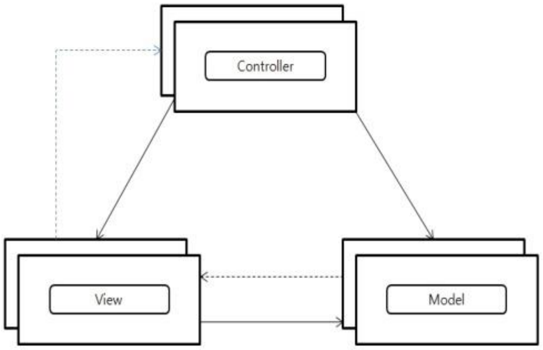

Figure 4. MVC Pattern

In MVC, “Model” indicates the application's data. “View” is the user interface element. “Controller” manages mutual interactions between the data and the business logic. The MVC pattern is structured using all three.

3. Web based EHR security requirements

Figure 5 shows a diagram of the sharing of health information provided by OpenEHR. When a patient’s health information is used for a secondary usage or other purposes, the infringement risk relating to the medical information increases as the number of people who are aware of the patient’s private or personal information increases. In particular, this may cause serious problems if it is used by a person in a type of occupation for which the confidentiality obligation is not required [10]. Nevertheless, the sharing of medical information can prevent duplicate checkups and repeated medical action. Therefore, personal medical information should be shared safely and the infringement of patient privacy should be prevented.

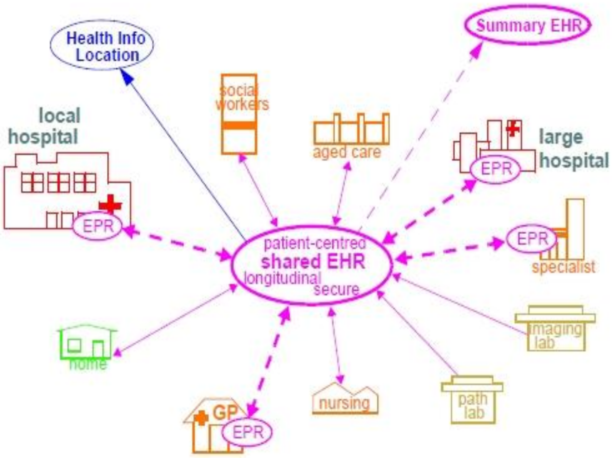

Figure 5. Patient-centred shared EHRs and the risk of patient medical information infringement [8]

When sensitive personal medical information is kept in a database in a medical institution, the maintenance of confidentiality from insiders and outsiders is necessary. Protection and access rights management for the privacy of patients and their history of medical service are also needed. In other words, for activation of the Healthcare service using the internet, protection of confidentiality of real time shared information, access rights control technology, *etc.*, are required. When considering a patient's privacy or personal information, protection is required. Furthermore, it is possible to make personal services based on shared medical data drawn from the EHRs. In particular, we can receive a great deal of context information (we define context information from smartphones as many sensing DBs of gravity sensing, accelerometer sensing, illumination sensing, near-sensing, and gyroscope sensing) from sensors that are carried in patients' and doctors' smart-phones. To use this method safely, a plan which guarantees the confidentiality and integrity of medical data should be suggested.

3.1 Encryption

In an e-Healthcare database system, when, where, and who accesses which and whose information should be precisely controlled. The access also should be traceable. Therefore, the right management for access control should be differentiated by such attributes as ID, location, time, *etc.*

A system for the searching and usage of medical information should also provide access control or anonymity based on the access history information or security policy to permit search. It is because the access right to medical information for treatment, for clinical research, or for education purposes may vary even in the case of the same employee's access to the same patient's information.

Not only is rights-based access control and privilege management for medical database important, but encryption functionality is also very critical. Therefore, the problem of a security mechanism for the safe management of health data must be resolved. The development of an encryption primitive for the medical data is required. A description of the cipher primitive is as follows.

- ABE (Attribute-Based Encryption): ABE is an attribute-based cipher. As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level (*i.e.*, by giving another party your private key) [11]. Medical information includes various attributes such as the biometrics of the patient, the location and time of medical events, etc. It is a type that can conduct decoding when the patient's several attributes match. It is a type based on the user's context, and encoding and decoding is possible using various attributes at any place and any time.

- PRE (Proxy Re-Encryption): PRE is a method that encrypts with the re-encryption key. A content owner publishes encrypted content in the form of a many-reader, single-writer file system. The owner encrypts blocks of content with unique, symmetric content keys [12]. PRE uses the cipher text encrypted by the public key of the authorizing person. Decoding is possible using an authorized person's password. In Re-Encryption, the proxy encrypts without decoding the cipher text of the authorizing person. Re-Encryption protects the password of the authorizing person.

3.2 Access Control

We now examine access rights management that can improve accessibility to health data in the e-Healthcare environment and maintain freedom in access control depending on an employee's role and history.

RBAC (Role Based Access Control) is access control based on the user's assigned role. Users are assigned with roles defined by certain rights and authority and are able to access and perform the task by the relationship with the assigned role.

By realizing access control in accordance with the assigned role in an EHR-using institution, systemic control of access is possible. However, utilizing RBAC, more flexible access control management is possible. It can also realize a Fine-grained Access Control function through open control based on policy or the relationship among the users.

4. EHR Security Management Model

This model is constructed based on OpenEHR. Figure 6 shows the structure of the EHR security management model.

Explanation about the specifics is as follows. The EHR security management model extracts XML through the Archetype Editor provided by Ocean Informatics. When it is web-based, it is viewed in a web browser through an XML parser. Here, the information saved in database uses a Java based cipher primitive. The process above is developed based on the MVC pattern. Each cipher primitive applies the mechanism that is mentioned in the EHR security requirements.

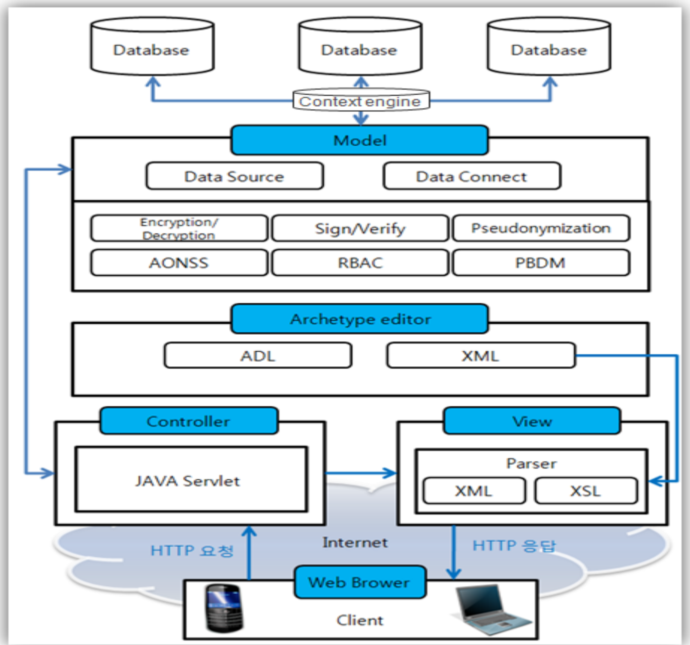

Figure 6. EHR security management mode

- The explanation about each module of the model is as follows.

- Web Browser: It functions as the client that can be connected through a PC, laptop computer, smart-phone, *etc.*

- View: It parses the required query into an XML document and XSL. It prints the output to the web browsers of the medical staff and the patient.

- Controller: It requests Model to process the requested query from the client (patient or medical staff). It delivers the requested results to View.

- Archetype Editor: It adds or corrects Archetypes provided by OpenEHR. It writes an XML document.

- Model: It performs the encryption of data, decoding, secret sharing, etc. in the Security/Privacy Sub-component (Encryption/Decryption, Sign/Verify, Pseudonymization, AONSS, RBAC, PBDM) in order to apply cipher Primitives needed for the requested controller and the EHR service mentioned above.

- Context Engine: It combines the various attributes information of patient. It determines the limit and sharing level for patient information based on privacy sensitivity. Privacy sensitivity is processed by a weighted algorithm for the attributes of patient information. It uses a Privacy/Security mechanism based on the patient's attributes.

- Database: It is the physical database where the data is stored by the user's request. It stores the sensitive attribute information of a patient separately according to its importance.

- Each module can be mapped out easily and rapidly by Archetype Editor which follows international standards. In particular, it helps to realize a system, as shown in Figure 7, which is optimized to contexts - aged care, medical specialist, large hospital, nursing, managing lab, social workers, health information location, local hospital, home, path lab - about medical information already contemplated in Figure 6. Context Engine is helpful in making decisions on the method and protection level of privacy from scattered medical information databases.

- During the process of implementing the system, it should be possible to share subtle medical data through a security-concerned mapping. Additionally, a realization of the context engine, *i.e.*, sensing such context as patient and doctor from a smart-phone in real time, is needed. The smart-phone is a huge collection of sensors such as gravity sensing, accelerometer sensing, illumination sensing, near-sensing, and gyroscope sensing as apart from the GPS receiving location under the user's privacy and personal information agreement.

5. Conclusions

Our research addresses the topic of modeling a secure Electronic Health Record (EHR) information system based on existing models of the OpenEHR initiative, the well-known model-view-controller (MVC) architectural pattern and the security requirements identified for medical information systems.

OpenEHR shows a standard proposal for Architecture [14]. This paper suggests a security model based on the MVC pattern of the EHR system. Therefore, a web service model is being developed by standardizing XML and web service security guideline.

The EHR service has efficiency when the medical staff's participating, sharing and opening of patients' health information is possible. Therefore, a security guideline that follows the standard of Architecture at a web service model based on EHR is necessary. In contrast, in the OpenEHR Architecture published so far, specific models and details that can satisfy various security requirements are not described. We are analyzing the security requirements of a web-based EHR system.

Throughout this report, we have proposed a new service of combining blood pressure information and a smart-phone's sensor as a specific case study. The proposed model will help to suggest an overall constituent module for the secured implementation of sharing various medical data regarding blood pressure and communications, as well as to identify their interactions.

This paper describes the component composition of the MVC Model, and modification and improvement of the Interface and MVC pattern. The foregoing can contribute to the realization of an EHR system that considers security in a detailed module.

Acknowledgments

This work was supported by the MKE (Ministry of Knowledge Economy) [A004700008], Development of realistic sense transmission system with media gateway supporting multi-media and multi-device.

References

[1] http://www.oceaninformatics.com/about-ocean/Overview.html, **(2011)**.

[2] K. Sadahiko, "Introduction to openEHR", Segaia Meeting, **(2009)** May 15.

[3] "Health Informatics - Requirements for an electronic health record architecture", ISO TS 18308:2004, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=52823, **(2011)** May.

[4] S. -J. Yoo, "Review report of EHR Architecture related International Standards", EHR Business Association, NH-ICT, **(2006)**.

[5] B. Blobel, "Advanced and secure architectural EHR approaches", Int J Med Inform., vol. 75, no. 3-4, **(2006)**, pp. 185-90.

[6] Y. M. Satria and K. Sadahiko, "Study on Electronic Health Record for use by Private Emergency Medical Service (EMS) in Indonesia - A case study of EHR in developing countries-".

[7] "Ocen Informatics Archetype Editor", https://projects.oceaninformatics.com/confluence/display/TTL/Archetype+Editor.

[8] T. Beale and S. Heard, "The openEHR EHR Service Model", The openEHR foundation, **(2003)**.

[9] A. Shamir, "How to share a secret", Communications of the ACM, vol. 22, no. 11, **(1979)**, pp. 612–613, doi:10.1145/359168.359176.

[10] O. Dunkelman, N. Keller and A. Shamir, "A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony", CRYPTO, (2010), pp. 393-410.

[11] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", In ACM Conf. Computer and Comm. Security, **(2006)**.

[12] G. Ateniese, K. Fu, M. Green and S. Hohenberger, "Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage", ACM Transactions on Information and System Security, vol. 9, no. 1, **(2006)** February, pp. 19.

[13] M. Fatemi, T. Eghlidos and M. Aref, "A Multi-stage Secret Sharing Scheme Using All-or-Nothing Transform Approach", Information and Communications Security Lecture Notes in Computer Science, vol. 5927/2009, **(2009)**, pp. 449-458, DOI: 10.1007/978-3-642-11145-7_35.

[14] http://www.connectingforhealth.nhs.uk, **(2011)**.

[15] http://www.openehr.org/releases/1.0.1/architecture/overview.pdf , 9/87 slide Figure 1 and 77/87 slide Figure 37, **(2011)**.

[16] http://www.openehr.org/wiki/display/healthmod/Archetypes+and+Terminology, **(2011)**.

[17] R. Chen, G. O. Klein, E. Sundvall, D. Karlsson and H. Ahlfeldt, "Archetype-based conversion of EHR content models: pilot experience with a regional EHR system", BMC Medical Informatics and Decision Making, vol. 9, pp. 1, http://www.biomedcentral.com/1472-6947/9/33, **(2011)**.

[18] http://www.openehr.org/knowledge, **(2011)**.

[19] http://www.slideshare.net/ysatria/open-standard-ehr-with-open-source-based-web-development, 7-8/14, **(2011)**.