CPR 시큐리티 시스템에 관한 연구*

김 석 수**

요 약

본 논문은 유비쿼터스환경에 실현되는 CPR(Computer-based patient record) 시스템에 관한 연구이며, CPR 시스템내에 시큐리티 시스템을 설계하고 분석하여 시큐리티 정책을 안정화 하기 위한 목적이다. 본 논문에서는 유비쿼터스 환경의 사용자를 고려한 CPR 시스템을 위한 개략적 설계를 하고 보안시스템 개발을 위해서 먼저 운용환경 및 보안 취약성 분석을 통해 CPR 시스템에서 필요한 보안 정책을 수립하고 이를 수행하기 위한 보안 시스템을 설계하였다. CPR 시스템을 지원하는 보안 시스템은 인증 시스템, 의료 정보의 XML 문서화 및 암호화, 네트워크 보안 시스템으로 구성된다.

A Study on the CPR Security System*

Seok-Soo Kim**

ABSTRACT

This paper proposes CPR(Computer-based patient record) system that is utilized in Ubiquitous environment, establish security policy by analyzing security limitation of system and design suitable security system in CPR system. The present study designed a CPR system and, for the development of a security system, established security policies for the CPR system through analyzing the operating environment and vulnerability in security and designed a security system implementing the policies. The security system supporting CPR system is composed of authentication system, XML documentation and encryption of medical information and network security system.

Key words : CPR, Security, XML, Network, Telemedicine

* This work was supported by a grant No. (R12-2003-004-03003-0) from Ministry of Commerce, Industry and Energy.

** 한남대학교 멀티미디어학부

1. Introduction

CPR system is a medical information system developed to make patients' medical information available to any hospital or health institution at any time. It analyzes the occurrence and flow of medical information related to patients, identifies substantial entities in the process of medical treatments, and builds logical data structure based on relations among the entities. However, because current CPR system provides information in batch mode through collective data management, it has difficulties in active processing of entity relations applied during the processing of medical information. Moreover, CPR system is mostly implemented in the client/server structure in storing and providing information, so it is exposed to the risk of information leakage by system users or unauthorized users. Information leakage may worsen people's perception on medical information system, which is based on patients' trust. Thus the present study examines how to apply the procedure of medical information processing to information effectively and designs the operating environment of CPR system fit for ubiquitous environment. In addition, we propose a security system for creating safe operating environment of CPR system in ubiquitous environment. The proposed CPR system is composed of user authentication system for access control over patient information, data encryption system for the integrity and confidentiality of important data, and encrypted communication system for each system unit for secure communication between servers and clients.

2. EMR System

2.1 Analysis of EMR system

This section analyzes EMR, which, among the medical information system, is the base technology of CPR.

Data capture function. This function is a document and image processing technology handling various forms of medical records and it includes DIP (Digital Image Processing) and medical image information system

Storage function. This means the storageof physical data, setting data standards, classifying and storing data, and keeping backup data.

Information processing function. This function is to process available data and produce useful information.

Information communication function. This enables the exchange and sharing of data. For this function, national or international standards should be set.

Security function. This function keeps data from unauthorized access.

Information presentation function. This function prepares stored data in the form of presentation.

EMR has the following basic functions and is being extended in a way of digitalizing hospital

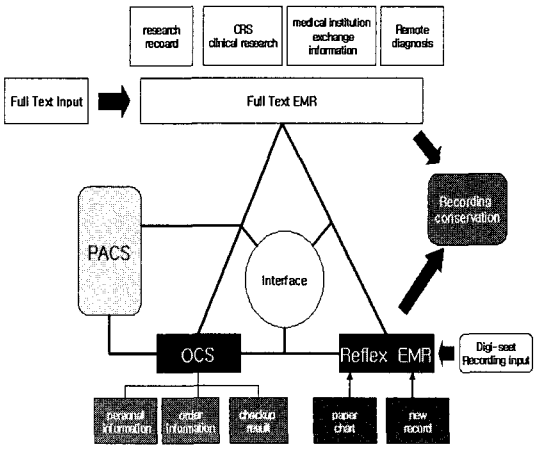
medical records by including additional technologies such as EMR (Electronic Patient Record) system.

2.2 Structure of EMR system

Most EMR systems in Korea are being operated together with EPR system, which is for effective computerization of existing work processes. EPR scan charts and utilize the image data as medical information. With the system, information can be input in text format or, if it is not easy, is scanned. On the contrary, EMR is a tool directly applicable to doctors' decision making, assisting theirmemory. It is used as an essential base for the accumulation of clinical experiences and knowledge and the performance of role research and clinical studies. As it overcomes problems in paper record and its maintenance, it is being actively utilized in maintaining and viewing records in network environment and recently as OCS and in exchanging information with insurance companies.

For the effective utilization of EMR system, it should contain all data related to patients including their case history, physical examination, diagnosis and interventions. Becauseit is difficult to digitalize the extensive volume of existing medical charts, however, records since the introduction of computer system are stored in text and those before the introduction are stored in image. Because of this, EMR system has a structure as in (Figure 1).

(Figure 1)shows how to apply medical information, which is hard to digitalize, to EMR system effectively. According to the figure, most of medical information in EMR system is text-based and is used in the presentation of medical records, CRS, clinical research, information exchange among medical institutions, remote diagnosis, etc. OCS is used in computerizing information on individuals, prescriptions and test results, and image EMR is used in managing charts in the past as well as new medical information. Moreover, PACS is used to process and store patients' precise diagnosis images. All these are integrated to form an efficient EMR system



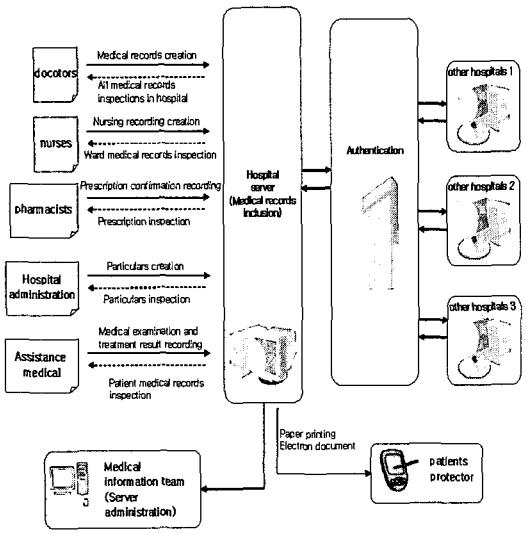
(Figure 1) Functional structure of EMR system

3. Design of CPR System in Ubiquitous Environment

3.1 Operating environment of CPR system in ubiquitous environment

For higher efficiency of CPR system in ubiquitous environment, information should be shared through intero peration with existing EMR system. This is a method of using legacy

systems. In addition, thesystem includes POC system in order to provide information to patients and their carers at any time and in any place and, by doing so, increase the utilization of the system in ubiquitous environment.Components of CPR system in ubiquitous environment are as in (Figure 2) and operations among the components are as follows.



(Figure 2) Components of CPR system in ubiquitous environment

The hospital server is a management server of the concept of existing EMR for managing electronic medical records. It receives information from doctors, nurses, pharmacists, the administration office of hospitals and auxiliarymedical institutions, and stores, manages and provides it real-time.

The authentication agency controls network connection and information security based on certificates for patient information sharing among the corresponding hospital and other hospitals. The servers of other hospitals are also management servers for the hospitals, composed of their own EMR system, and medical information is transmitted between the hospitals and patients via the authentication agency. All hospital servers include an information service system for patients through the wireless Internet.

3.2 Data of CPR system in ubiquitous environment

In CPR system, data includes important information such as patients' and doctors' personal information and critical medical technologies, so it must be protected securely. Information used in the system is largely divided into personal information, medical technology information, hospital information, etc. Particularly because personal information contains individuals' personal details, it must be protected carefully. In general CPR information management is all saved in one database and managed through DBMS (Database Management System). The integrated management gives the effect of consistent information management but, if the volume of information becomes huge, performance may go down, any accidental information leakage may bring about serious results and the system can be a conspicuous target of hackers' attack. Thus, the data of CPR system in ubiquitous environment must be under primary integrated management by the EMR server of each hospital, and the risk of information leakage needs to be distributed by providing each user with objectified information based on XML (Extensible Markup Language). Objectified personal medical information prompts real-time update of changes, and effectively structures data through logical analysis of entity

relations among data during data processing.

4. Security Policies of CPR system in Ubiquitous Environment

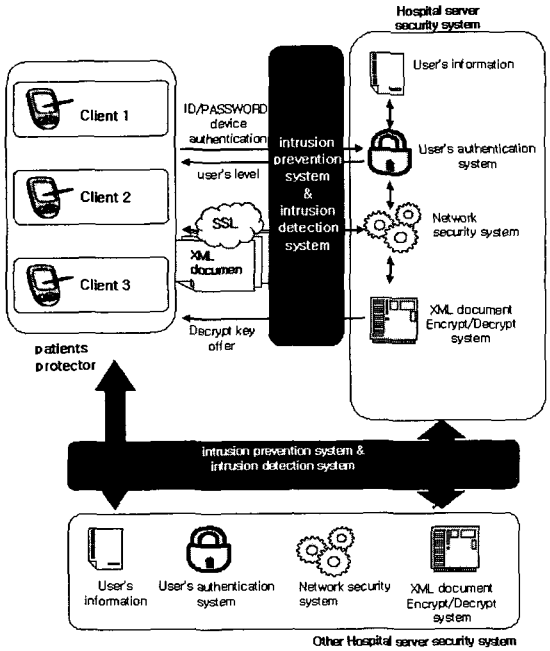
CPR system is a global trend, and the Internet and medical information sharing system such as remote diagnosis are prevailing throughout the medical world. In this situation, various types of sensitive patient information can spread in a moment to the world. That is, due the possibility of the abuse of medical information, each country is tightening information security and several legal issues are rising [1]. Thus, in response to the vulnerability of security analyzed in the previous section, CPR system requires the establishment of security policies concerning the following aspects : Authentication/access control, Confident iality/integrity, Non-repudiation, Avail ability.

In response to risk factors threatening security as presented in the previous section, we need technical security measures as follows.

First, user authentication system should be introduced. User authentication mechanism can be implemented using ID/password, one-time password, two-factor authentication, open key certificate, etc. CPR should intensify its authentication system using ID and password for protecting information of personal mobile terminal users in ubiquitous environment. Information service through the wireless Internet is exposed to various security risks compared to wired service [2]. In this study, we use two-factor authentication for stricter authentication. Two-factor authentication provides intensified user authentication by adding the authentication of equipment or device such as PC, laptop or portable device (cellular phone, PDA) in addition to ID and password. Second, XML is used as recommended by HL7 (Health Level 7) to share information among heterogeneous EMR systems and build integrated environment for protecting information [3]. For convenient exchange of information among systems, transformed medical information documents are developed fittingly to Web environment. Moreover, security for XML documents using XML encryption algorithm SOAP (Simple Object Access Protocol) and network security using SSL (Secure Sockets Layer) are applied together. Third, security level is defined for user information, and XML documents are partially encrypted to restrict the disclosure of the documents according to users. Fourth, in order to complement/monitor vulnerability in the integrity and confidentiality of data exchanged between CPR systems, each user's access to and use of information is logged and analyzed. Fifth, intrusion detection and prevention system is introduced in preparation against hackers' intrusions and DOS attacks.

5. Structure of CPR Security System in Ubiquitous Environment

This chapter designs CPR security system to provide independent security service in various CPR application program environments based on the security policies of CPR system in ubiquitous environment as established in Chapter 4. CPR security system is composed of user authentication, encryption and network security system as in (Figure 3).

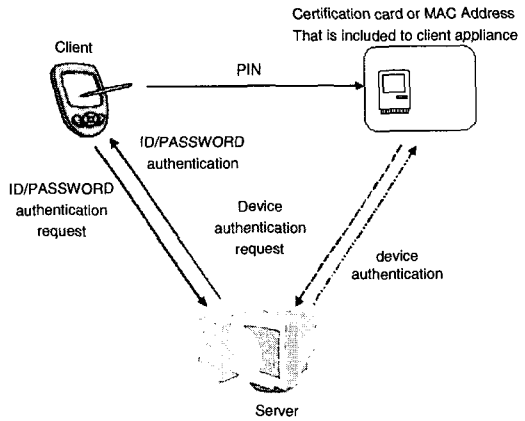


(Figure 3) Structure of CPR security system

A patient or a carer accesses a hospital server using his/her mobile terminal. The hospital server uses two-factor authentication to identify the user. That is, user authentication is carried out with ID/password and device authentication and then the user's level is confirmed. If authentication is completed properly, the server and the user send/receive information. All information is exchanged in XML and is encrypted through XML security algorithm and SOAP according to user level. In addition, network security is provided through SSL. In information exchange between the user and other hospital servers and between hospital servers, two-factor authentication is applied first and then security for information itself is applied. The process of information request and provision between a hospital server and a patient and between two hospital servers is monitored by the intrusion detection and prevention system and the data is used in log analysis for each user and system

5.1 Two-factor authentication system for user authentication

The user authentication system provides functions to control users' access and their access right. The ID/password method is convenient for users but it is exposed to a high risk of exposure. 'One-time password management system' is an improvement of 'ID/password management system,' providing stricter authentication compared to the former method that users have to enter ID and password whenever they access the system, but it requires frequent changes of password and its management is complicated. Thus, the present study proposes two-factor authentication as a convenient and accurate authentication method. Two factor authentication demands more accurate authentication by verifying the device used in communication in addition to ID and password.



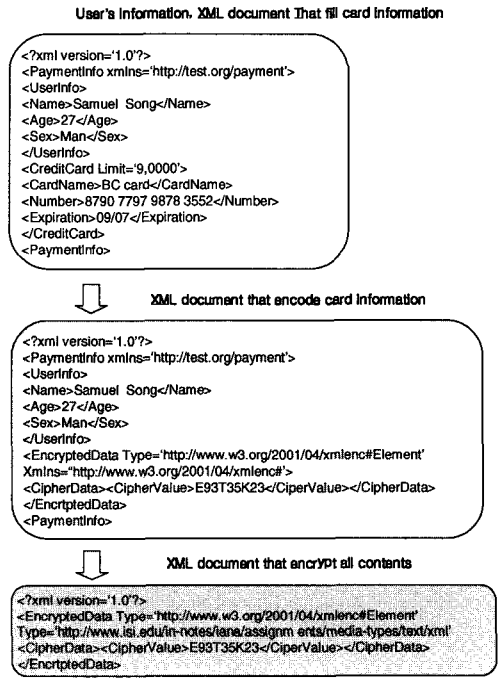
(Figure 4) Two-Factor Authentication

(Figure 4) describes the two-factor authentication protocol. Two-factor authentication first verifies the users basic information and then verifies the machine used based on the verification card (smart card) contained in the machine or the MAC address of the machine.

5.2 XML security for user authentication

In addition to two-factor authentication system, we need a security system to encrypt XML documents and provide them differently according to user level. For the encryption of XML documents, a module should be designed based on XML signature standard [4, 5] and XML encryption standard [6, 7]. The purpose of module design is to remove the problem that the accuracy of the operation of XML security on domestic standard algorithms and encryption libraries has not been proved. Depending on necessity, XML security technologies can encrypt information partially. XML documents can be encrypted differently according to the importance of information or whether the information is open or confidential and the whole document can be encrypted by the user's request. In this way, XML security encrypts and decrypts information selectively and this improves system performance and can meet users requirements.

(Figure 5) shows the process of preparing an XML document through partial encryption. The document is divided into user information and payment information. The figure shows the encryption of only card information in the payment part and that of the whole document.



(Figure 5) XML document resulting from partial encryption

6. Conclusions and tasks for future research

The present study designed a CPR system and, for the development of a security system, established security policies for the CPR system through analyzing the operating environment and vulnerability in security and designed a security system implementing the policies. The security system supporting CPR system is composed of authentication system, XML documentation and encryption of medical information and network security system.

The designed CPR security system is expected to provide information service more safely as it

uses two-factor authentication to identify users in POC environment where medical information is provided through mobile terminals in ubiquitous environment.

Further studies should be made in the future for more secure information protection in wireless communication by integrating, extending and applying safe authentication system, intrusion prevention system, intrusion detection system, etc. and through inter operation with newly emerging devices with the implementation of perfect security system and the development of ubiquitous environment.

References

[1] Jeong hyeon cheol, "medical information system of security", Communications of the Korea Information Science Society, Vol. 16, No. 12, 1998.

[2] Mishra, A., and rbaugh, W. "An Initial Security Analysis of the IEEE 802.1X Standard", February, 2002.

[3] HL7,http://www.hl7.org/Press/20040427b.pdf IETF/W3C, "XML-Signature Requirements (Working Draft)", Oct. 1999.

[4] http://www.w3.org/TR/1999/WD-xmldsig-requirements-19991014.html

[5] IETF/W3C, XML-Signature Syntax and Processing(Working Draft), Oct. 2000, http://www.w3.org/TR/2000/WD-xmldsig-core-20001012/

[6] W3C XML Encryption WG, "XML Encryption Charter," http://www.w3.org, 2001.

[7] xml-encrytion@w3.org Mail Archives, http://lists.w3.org/Archives/Public/xml-encryption/

김 석 수

1991년 성균관대학교 대학원 정보공학과 공학석사
1991년~1996년 정풍물산(주) 중앙연구소 주임연구원
1997년~1998년 (주)한국탑웨어 책임연구원
2002년 성균관대학교 대학원 공학박사
1998년~2000년 경남도립거창전문대학 교수
2000년~2003년 동양대학교 컴퓨터공학부 교수
2003년~현재 한남대학교 멀티미디어학과 교수