Journal of Digital Contents Society Vol. 11 No. 2 Jun. 2010(pp. 135-144)

전자의무기록 변경 방지 프로토콜

주한규*

요 약

의무기록은 의료행위에 대한 매우 중요한 기록으로 임의로 변경되지 말아야 한다. 현존하는 의무기록은 모두 변경될 수 있는 여지가 있다. 정보기술의 발달로 전자의무기록이 점차 널리 사용되게 되었다. 전자의무기록을 사용함에따라 암호학적 기반을 이용하여 의무기록 변경을 방지할 수 기법을 사용할 수 있다.

본 논문에서는 연결해쉬, 전자서명, 전자공증 등의 암호학적 기법을 이용하여 의무기록 변경을 방지할 수 있는 기법을 제안하고 프로토타입을 통하여 수행을 분석한다. 제안된 기법은 적은 추가비용으로 의무기록 변경을 현실적으로 불가능하도록 한다.

Electronic Medical Record Modification Prevention Protocol

Hankyu Joo*

Abstract

Medical records are very important records and should not be modified after creation. The current medical records are liable to improper modification. With the development of information technology, electronic medical records (EMR) are used widely. For the EMR, cryptographic primitives may be used to develop techniques to prevent medical record modofication.

In this research, a technique to prevent improper medical record prevention is proposed. It uses crytographic primitives such as linked hash, digital signature, and electronic notarization. A prototype system is also developed for performance analysis. The proposed method makes the medical record modification impossible with a small amount of additional cost.

Keywords : 전자의무기록, 신뢰성, 해쉬, 전자서명, 전자공증

1. 서론

해마다 많은 수의 의료분쟁이 발생하며 그 수는 매년 증가해 온 것으로 알려졌다. 소비자원에서 처리한 의료분쟁 건수가 1999년 271건에서 2005년에는 1093건으로 7년 사이 4배가 급증하였으며 이러한 추세가 지속된다면 의료분쟁 건수가 급격히 증가할 것으로 예견된다 [1].

의료 분쟁이 발생하는 경우 의무기록은 중요한 증거 자료가 된다[2]. 의무기록은 작성 이후 법에서 정한 기간 동안 의료기관에 보관되며 변조되지 말아야 한다. 의무기록은 전통적으로 의료인에 의하여 종이 문서에 작성되고 서명을 첨부하였다. 근래에 들어 컴퓨터의 도입으로 전자의무기록(Electronic Medical Record, EMR)의 사용이 증가하고 있으며 이 경우 의료인의 전자서명이 전자의무기록에 첨부된다.

현재 사용되는 기법은 의료기관 내에서 의무기록을 변조할 수 있는 여지를 남겨두고 있다. 종이의무기록의 경우, 현재 존재하는 의무기록을 폐기하고 새로운 의무기록을 작성한 후 의료인이 서명할 수 있으므로 쉽게 변경할 수 있다. 전자의무기록의 경우에도 해당 기록을 삭제한 후 새로운 의무기록을 생성하고 의료인이 새로운 의무기록에 전자서명을 첨부할 수 있으므로 쉽게 변경할 수 있다.

본 논문에서는 과다한 부가적인 비용 없이 신뢰할 수 있는 의무기록을 생성할 수 있는 기법

※ 제일저자(First Author) : 주한규
접수일:2010년 03월 12일, 수정일:2010년 06월 26일, 완료일:2010년 06월 29일
* 한림대학교 부교수
hkjoo@hallym.ac.kr

을 제안한다. 의료기관은 신뢰성 있는 의무기록을 제공함으로써 의료분쟁 시 논란을 피할 수 있을 것이다.

본 논문의 구성은 2절에서는 관련 연구를 기술하고 3절에서는 전자의무기록의 신뢰성 증진 기법을 제안한다. 4절에서는 프로토타입 설계가 기술되고 5절에서 제안된 기법에 대한 분석과 고찰이 기술되고 6절에서는 결론이 기술된다.

2. 관련연구

2.1. 관련 지침 및 제품

의료법에 의하면 의료인은 각각 진료기록부, 조산기록부, 간호기록부, 그 밖의 진료에 관한 기록을 갖추어 두고 그 의료행위에 관한 사항과 의견을 상세히 기록하고 서명하여야 한다. 또한 의료인 또는 의료기관의 개설자는 보건복지가족부령으로 정하는 바에 따라 이를 보존하여야 한다[3].

전자의무기록은 전자문서 형태의 의무기록이며 종이의무기록에 비교하여 긍정적인 효과가 나타나고 있다[4]. 의료법에서는 전자의무기록을 허용하며 다음과 같이 기술한다. 의료인이나 의료기관 개설자는 진료기록부 등을 전자서명법[5]에 따른 전자서명이 기재된 전자문서(전자의무기록)로 작성, 보관할 수 있다. 의료인이나 의료기관 개설자는 보건복지가족부령으로 정하는 바에 따라 이를 안전하게 관리, 보존하는 데에 필요한 시설과 장비를 갖추어야 한다. 그리고 누구든지 정당한 사유 없이 전자의무기록에 저장된 개인정보를 탐지하거나 누출, 변조 또는 훼손하여서는 안된다[3]. 또한 의료법 시행규칙에 따르면 의료인이나 의료기관의 개설자는 전자의무기록을 안전하게 관리·보존하기 위하여 전자의무기록의 생성과 전자서명을 검증할 수 있는 장비와 전자서명이 있은 후 전자의무기록의 변경 여부를 확인할 수 있는 장비를 갖추어야 한다고 명시하고 있다[6].

전자서명법에서는 다른 법령에서 문서 또는 서면에 서명, 서명날인 또는 기명날인을 요하는 경우 전자문서에 공인전자서명이 있는 때에는 이를 충족한 것으로 본다. 또한 공인전자서명이 있는 경우에는 당해 전자서명이 서명자의 서명, 서명날인 또는 기명날인이고, 당해 전자문서가 전자서명된 후 그 내용이 변경되지 아니하였다고 추정한다고 명시하고 있다[5]. 보건산업진흥원에서 전자의무기록에 대한 공인전자서명 적용 지침을 개발하였으며 이에서 전자의무기록의 법적 보호를 위하여 전자의무기록에 공인전자서명 첨부하라고 기재하고 있다[7, 8].

현재 많은 수의 전자의무기록 시스템이 개발되어 사용되고 있다[9, 10 11]. 이들 시스템은 공통적으로 공인전자서명 기능을 지원한다. 공인전자서명을 위하여 의료인은 전자서명을 위한 공개키/개인키 쌍을 생성하여 공인인증기관으로부터 공개키에 대한 공인인증서를 발급받는다. 매번 진료기록을 입력할 때 의료인은 자신이 입력한 진료기록에 자신의 개인키를 이용하여 전자서명을 수행하며, 전자서명이 첨부된 진료기록은 의료기관의 데이터베이스에 저장된다. 공인인증서를 이용한 전자서명을 첨부한 진료기록은 법적으로 종이를 이용한 의무기록과 동일한 효력을 갖는다.

2.2. 문제점 분석

현재 존재하는 의무기록은 작성 이후 변경이 가능하며 이는 의료분쟁 시 논란을 유발시킨다. 종이의무기록의 경우 의료인과 의무기관이 공모하는 경우 의료인이 해당 의무기록을 폐기한 후 새로운 의무기록을 작성하고 서명할 수 있으므로 변경의 여지가 있다.

전자의무기록에 대한 공인전자서명 적용 지침과 현재 사용되는 전자의무기록 시스템의 경우 의료인의 전자서명을 첨부함으로써 의무기록이 작성 후 변조되지 않은 곳으로 추정한다. 그러나 의료인의 전자서명이 첨부된 전자의무기록의 경우에도 의료인과 의료기관이 공모하는 경우 기존의 의무기록을 삭제한 후 새롭게 작성된 의무기록에 의료인이 다시 전자서명 할 수 있으므로 변경의 여지가 있다. 이는 전자서명이 있은 후 전자의무기록의 변경 여부를 확인할 수 있는 장비를 갖추어야 한다고 명시하고 있는 의료법 시행규칙[6]에도 위배된다.

이에 대한 대책으로 환자가 모든 의무기록에 대한 사본을 유지하도록 하거나 매 의무기록에 신뢰할 수 있는 제 3 자의 서명을 첨부하여 신뢰할 수 있는 의무기록을 작성할 수 있겠지만

과다한 불편 또는 비용이 필요하므로 현실적으로 불가능 하다.

3. 변경 방지 기법

3.1. 수행환경

본 연구에서 제안되는 기법의 참여자는 의료인, 의료기관, 그리고 공증기관이다. 의료기관은 의료 행위를 행하는 기관으로 병원이 이에 해당한다. 의료인은 의료기관에 종사하는 종사자로 의사, 간호사 등이 이에 해당한다. 공증기관은 공인인증기관, 지역 보건소, 지방자치행정기관 등 환자와 병원의 중립적 위치에 있는 신뢰할 수 있는 기관이 될 수 있다.

의료인은 환자를 진료하며 의무기록을 작성(입력)한다. 작성한 의무기록에 전자서명을 하여 본인이 작성한 의무기록임을 명확히 한다. 전자서명을 위한 공개키/개인키 쌍을 가지며 공개키는 공인 인증기관으로부터 인증서를 발부받는다.

각 의료기관은 의료인이 작성한 의무기록을 유지하는 책임이 있다. 의무 기록을 공증기관으로부터 공증을 받아 의무기록이 변조되지 않았음을 증명하는 역할 또한 수행한다. 주기적으로 의무기록에 대한 전자서명을 수행하며 이를 공증 기관으로부터 공증 받는다. 각 의료기관은 전자서명을 위한 기관 공개키/개인키 쌍을 가지고 있다. 기관 공개키는 공인인증기관으로부터 인증서를 발부받는다. 기관 공개키는 의료기관장 명의의 공개키일 수도 있다. 그러나 이는 개인적인 사용 용도의 공개키와 같지 않는 것이 효율적이다. 이는 기관의 직인과 같이 의료기관에서 신뢰하는 의료기관 종사자가 의료기관장 명의의 키를 이용하여 의료기관장을 대리하여 서명할 수 있기 때문이다.

공증기관은 환자와 병원의 중립적 위치에 있는 신뢰할 수 있는 기관으로 의료기관에서 의무기록에 대한 공증 요청이 있으면 공증을 수행하여준다. 공증을 위하여 전자서명을 하며 이를 위하여 공증기관의 공개키/개인키 쌍을 가지고 있으며 공개키는 공인인증기관으로부터 인증서를 발부받는다. 공증기관은 현재 존재하는 공적 기관, 예를 들어 공인인증기관 또는 정부기관 등, 이 수행할 수 있다.

3.2. 표기법

본 논문에서는 다음의 표기법이 사용된다.

- N: 공증기관
- M: 의료기관
- E: 의료인 (여러 명의 의료인 중 한 명을 나타내기 위하여 e_i, e_j 등으로도 표현됨)
- $H(n)$: 일방향 해쉬 함수 (입력은 메시지 n)
- c_i: 의료인에 의하여 작성된 의무기록, 첨자 i는 의료기관에 저장되는 순서를 의미
- $E_k(m)$: 메시지 m을 키 k를 이용하여 암호화
- $D_k(c)$: 암호문 c를 키 k를 이용하여 복호화
- $x \stackrel{?}{=} y$: x와 y의 동일성 확인
- $sign_A(m)$: 메시지 m에 대한 A(E, M, 또는 N)의 전자서명
- tS: 특정 시점의 시각(time stamp)
- $x \mid y$: x와 y의 연결(concatenation)

3.3. 접근 방법

의무기록을 변경하기 어렵게 하기 위하여 일방향 해쉬 함수[12, 13, 14]를 응용한 연결해쉬, 전자서명[12, 15, 16], 그리고 전자공증[17]을 사용한다.

3.3.1. 해쉬함수와 전자서명

일방향 해쉬 함수는 임의의 길이의 자료를 일정한 길이의 이진 코드로 바꾸어주는 함수이다. 일방향 해쉬 함수 $H(n)$ 은 일방향 속성을 가지고 있다. 즉, 주어진 자료 n 으로부터 $h = H(n)$ 을 만족하는 해쉬값 h 는 쉽게 구할 수 있으나, 주어진 해쉬값 h 로부터 $h = H(n)$ 을 만족하는 자료 n 을 구하는 것은 현실적으로 불가능하다. 일방향 해쉬 함수는 또한 충돌회피성의 속성을 가지고 있다. 즉 주어진 자료 n 이 있을 때 $H(n) = H(m)$ 을 만족하는 어떠한 m 을 찾는 것 또한 현실적으로 불가능하다.

MD5[13], SHA-1[14] 등이 널리 사용되는 해쉬 함수이다. MD5는 임의의 길이의 자료로부터 128 비트 길이의 해쉬값을 생성해내는 해쉬 함수 이다. SHA-1은 임의의 길이의 자료로부터 160 비트 길이의 해쉬값을 생성해내는 해쉬 함수 이다.

전자서명은 인증과 부인 방지 기능을 제공하는 암호학적 기법이다. 전자서명은 공개키 암호

에 기반을 둔 기법으로 수기 서명과 법적으로도 동일한 효력을 가진다[7]. 전자서명을 위한 키 생성 시에 공개키와 개인키 쌍을 생성하여 공개키는 외부에 공개하고 개인키는 본인만이 보관하여 외부에 알려지지 않도록 한다. 서명하고자 하는 전자문서에 자신의 개인키로 서명함으로써 서명을 할 수 있다. 전자문서에 대한 올바른 서명 첨부 여부를 서명자의 공개키를 이용하여 확인할 수 있다.

RSA[15]의 예로 보면 전자문서에 해쉬 함수를 적용시킨 후 이를 자신의 개인키를 이용하여 암호화함으로써 전자서명을 한다. 즉 A 가 공개키/개인키 쌍으로 (Pub_A, $Priv_A$)를 가지고 있을 때, 주어진 전자문서 m 에 대한 전자서명 S 를 생성하는 것은 다음과 같이 표현될 수 있다.

$$S = E_{PrivA}(H(m))$$

전자서명을 확인하는 경우, 확인하고자 하는 전자문서에 해쉬 함수를 적용한 값과 첨부된 전자서명을 서명자의 공개키로 복호화한 값이 동일하면 올바른 서명이다. 즉 A 의 공개키가 Pub_A 일 때, 주어진 전자문서 m 에 첨부된 전자서명 S 가 A 에 의해 서명되었는지 확인하는 것은 다음과 같다.

$$H(m) \stackrel{?}{=} D_{PubA}(S)$$

RSA[15], DSS[16]등이 전자서명에 일반적으로 사용된다.

3.3.2. 연결 해쉬

연결해쉬는 다음과 같이 정의된다.

$h_i=H(c_i \ / \ h_{i-1})$, *where* $i = 0, 1, 2, 3,...,$ *and* $h_0=IV$

즉, h_0 값은 임의의 초기값(IV)을 가진다. 매번 기록내용(c_i)이 작성될 때 해쉬값(h_i)이 계산되며, 이 해쉬값은 현재의 기록내용(c_i)에 이전 해쉬값(h_{i-1})을 연결한 값($c_i \ / \ h_{i-1}$)에 해쉬함수를 적용한 값이 된다. 이와 같이 해쉬체인을 사용하면 하나의 기록내용 c_j를 변경하면 그 이후의 모든 해쉬값(h_k, *where* $k \geq j$)이 변경되어야 한다.

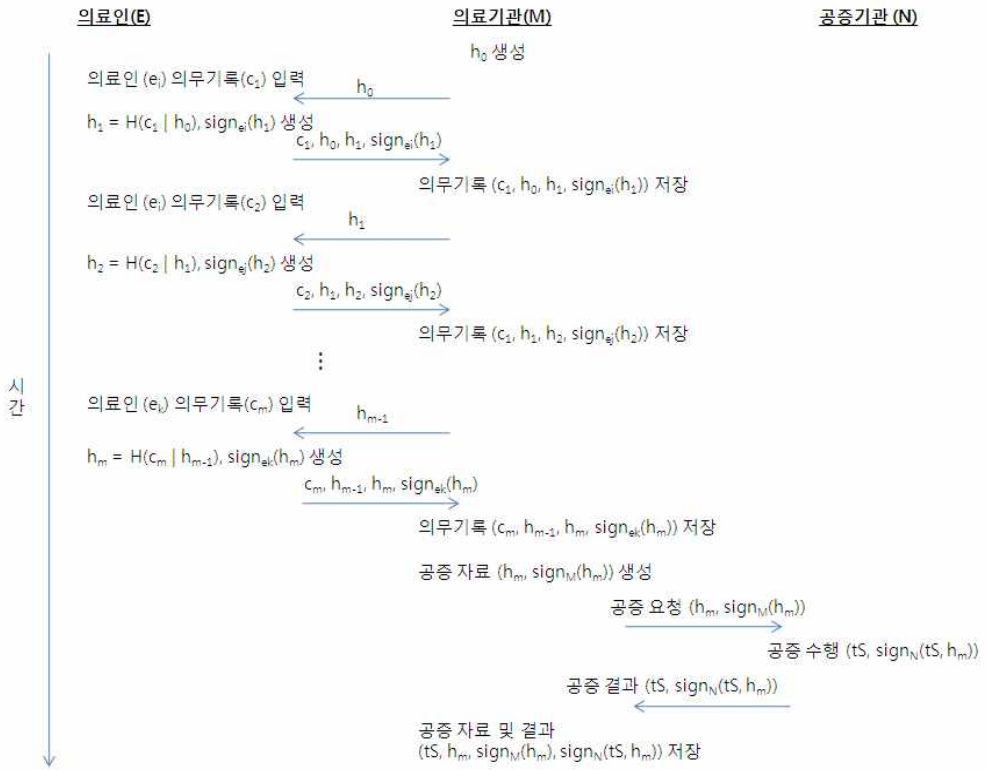
해쉬체인에 전자서명을 첨부하면 변경이 어려워진다. 즉 모든 해쉬값 h_i 에 전자서명을 한다고 하자. 만약 하나의 기록내용 c_j 를 변경하면 그 이후의 모든 해쉬값(h_k, *where* $k \geq j$)이 변경되어야하며 모든 변경된 해쉬값에 새로 전자서명을 수행하여야 한다. 만약 다수의 참가자가 기록을 입력하였으면 이들이 모두 다시 서명 하여야 변경이 가능하며 이는 또한 많은 시간을 필요로 함과 동시에 이들 모두가 추후 변경에 동의할 의사가 있어야 한다.

3.3.3. 전자공증

중립적이고 신뢰할 수 있는 제 3 자인 공증기관이 존재하는 경우 공증기관으로부터 공증을 득함으로 특정 자료의 신뢰성을 높일 수 있다. 전자공증의 경우, 공증 요청자는 공증을 필요로 하는 자료를 공증기관에 전송함으로써 공증을 요청하고 공증 기관은 자신의 비밀키를 이용하여 전자서명 함으로써 공증을 수행한다. 공증기관은 전자서명 시에 당시 시각(time stamp)을 첨부하여 특정 시각에 자료가 존재하였음을 증거할 수 있다. 공증 요청자의 경우 자료 전체를 전송하지 않고 자료의 해쉬값만 전송하여 공증을 요청할 수도 있으며 이 경우 자료에 대한 내용을 누출하지 않고도 공증을 획득할 수 있다. 현재 국내에서 공식적으로 시행되고 있지는 않으나 확립된 프로토콜은 존재한다[17].

3.3.4. 업무흐름

의료인은 전자의무기록시스템에 로그인함으로써 의무기록 입력이 가능하다. 의료인은 더 이상 입력할 내용이 없으면 로그아웃하여 작업을 종료할 수 있다. 의료인에 의하여 작성되고 서명된 의무기록은 의료기관의 컴퓨터에 저장되며 이러한 의무기록들은 주기적(예를 들어 60분)으로 공증기관으로부터 전자공증을 받음으로써 특정 시간 이후(최대 시간은 공증 주기)에는 의무기록 변경 가능성을 제거한다. 그리고 한 주기 내에서의 의무기록 변경을 어렵게 하기 위하여 연결 해쉬를 사용한다. 의료기관의 의료인이 기록 내용(의무기록)을 입력하고 연결 해쉬에 전자서명 하게 함으로써 의무기록의 변경을 어렵게 한다. 전자공증을 사용하여 공신력을 높일 수 있다. 주기적으로 연결해쉬에 의하여 생성된 해쉬



(그림 1) 업무 흐름

값을 신뢰할 수 있는 공증기관으로부터 공증을 받도록 하고 공증된 결과를 저장한다. 특정 시점에서의 마지막 해쉬값을 공증 받으면 그 이전의 모든 의무정보가 연결 해쉬에 의하여 연결되어 있으므로 그 시점 이전의 어떠한 의무정보도 공증 이후에 변경이 일어날 수 없다.

업무 흐름을 그림으로 나타내면 (그림 1)과 같다.

3.4. 상세 프로토콜

3.4.1. 수행 절차

의료기관에 저장되는 각 의무기록은 의무기록번호(*recNo*), 기록 내용(*contents*), 현 레코드와 연결된 이전 의무기록번호($recNo_{pre}$), 이전 의무기록의 해쉬값(h_{Pre}), 현 의무기록의 해쉬값(h), 그리고 전자서명(*sign*)으로 구성된다. 이를 그림으로 나타내면 (그림 2)와 같다.

recNo	contents	$recNo_{pre}$	h_{pre}	h_{recNo}	sign

(그림 2) 의무기록의 구조

의무기록번호(*recNo*)는 각 트랜잭션에 일련번호를 부여한 것으로 저장되는 순서에 따른다. 가장 처음에 입력되는 트랜잭션의 번호는 1번으로 초기화 한다. 의무기록번호는 특정 기간마다 초기화 될 수도 있다. 기록 내용(*contents*)은 의료인에 의하여 작성되는 환자에 대한 진단/처방 기록으로 의료인이 입력하는 내용이다. 기록 내용에는 의료인 등록번호, 의료인 성명, 진료 받은 이의 인적사항, 진단/치료 내역, 진료 당시의 시간 등이 포함된다. 이전 의무기록번호($recNo_{pre}$)는 현재 의무기록과 연결된 이전의 의무기록의 번호이다. 현재 의무기록번호가 j 이면 이전의무기록 번호는 $j-1$이 된다. 이전 트랜잭션 해쉬값(h_{pre})은 이전 의무기록에서 보관 중이 해쉬값이다. 해쉬값(h_{recNo})은 현재의 기록 내용과

직전의 트랜잭션 번호, 그리고 직전 트랜잭션의 해쉬값을 연결한 후 이에 해쉬 함수를 적용시킨 값이다. 전자서명(*sign*)은 이 해쉬값에 의료인의 개인키를 이용하여 전자서명한 결과가 된다.

의료인은 도전/응답 방식으로 의무시스템에 로그인할 수 있다. 로그인을 위하여 의료인(*E*)과 의료기관(*M*)은 다음과 같은 프로토콜을 수행한다.

$E \rightarrow M$: $login\_request$
$M \rightarrow E$: $random$
$E \rightarrow M$: $ID_E,\ sign_E(random)$

의료인이 로그인을 요청하면 의료기관은 임의의 정수(*random*)를 선택하여 도전한다. 의료인은 자신의 개인키를 이용하여 도전받은 정수에 서명함으로써 올바른 의료인임을 보인다. 의료기관은 받은 서명이 올바른 의료인의 서명임을 확인한다.

의무기록이 작성된 후 의무기록을 저장하기 위하여 의료인과 의료기관은 다음과 같은 프로토콜을 수행한다.

$E \rightarrow M$: $save\_request$
$M \rightarrow E$: $recNo_{pre},\ h_{pre}$
$E \rightarrow M$: $contents,\ recNo_{pre},\ h_{pre},\ h_{recNo},$
$sign_E(h_{recNo})$

의료인에 의하여 의무기록이 작성되면 의료기관에 저장 요청을 보낸다.

의료기관은 저장 요청 받은 순서에 따라 의무기록번호를 할당한다. 의료기관은 이전 의무기록번호와 이전 의무기록의 해쉬값을 의료인에게 전송한다. 초기 해쉬값(h_0)는 특정 초기 값, 예를 들면 *0*, 으로 초기화 한다.

의료인은 현재 의무기록의 해쉬값을 계산하고 이에 전자서명을 수행한다. 현재 의무기록의 해쉬값은 다음과 같이 계산된다.

$$h_{recNo} = H(contents \ / \ recNo_{pre} \ / \ h_{pre})$$

즉 현재 의무기록의 해쉬값은 의료인이 입력한 기록 내용과 이전 의무기록번호 그리고 이전 의무기록의 해쉬값을 연결한 값에 해쉬 함수를 적용시킨 결과가 된다. 전자서명은 현재 의무기록을 위하여 계산된 해쉬값에 의료인의 개인키를 이용하여 전자서명함으로써 생성한다. 의료인은 기록 내용, 이전 의무기록번호, 이전 의무기록 해쉬값, 현재 의무기록 해쉬값, 그리고 전자서명을 의료기관에 전송한다.

의료기관은 수신한 내용의 전자서명을 확인한다. 서명이 확인되면 할당된 현재 의무기록 번호와 함께 의무기록을 저장한다.

의료인은 더 이상 작업할 내용이 없으면 로그아웃하여 세션을 끝낼 수 있다. 일정 시간 의료인의 입력이 없을 경우 의료기관에서 임의로 세션을 종료할 수도 있다. 다음은 의료인이 의료기관에 보내는 로그아웃 요청 메시지를 보인다.

$E \rightarrow M$: $logout\_request$

의료기관(*M*)과 공증기관(*N*)은 일정 시간마다 (예를 들어 매 60분) 다음의 프로토콜을 수행하여 공증을 수행한다.

$M \rightarrow N$: $recNo,\ h_{recNo},$
$sign_M(recNo \ / \ h_{recNo})$
$N \rightarrow M$: $tS,\ sign_N(tS \ / \ recNo \ / \ h_{recNo})$

특정 시점이 되면 의료기관은 현재 후속 의무기록이 없는 마지막으로 저장된 의무기록의 의무기록번호(*recNo*)와 해당 의무기록의 해쉬값(h_{recNo}) 쌍, 그리고 그 쌍의 값에 의료기관의 개인키로 전자서명($sign_M(recNo \ / \ h_{recNo})$)하여 이를 공증기관에 전송함으로써 공증을 요청한다.

공증기관은 의료기관의 공개키로 서명을 확인하여 올바른 서명이면 공증기관의 개인키를 이용하여 요청 자료에 현재 시각(*tS*)을 첨부하여 전자서명($sign_N(tS \ / \ recNo \ / \ h_{recNo})$)한 후 현재의 시각(*tS*)과 함께 의료기관에 전송함으로써 공증을 수행한다.

의료기관은 공증기관으로부터 받은 정보를 보관한다. 보관된 정보는 특정 시점에 의료기관이 해쉬값을 공증기관으로부터 공증받았음을 의미하며 이는 특정 시점 이전에 기록된 어떠한 의무기록도 이후로는 변경되지 않았음을 증거하는 기록이 된다.

3.4.2. 확인 절차

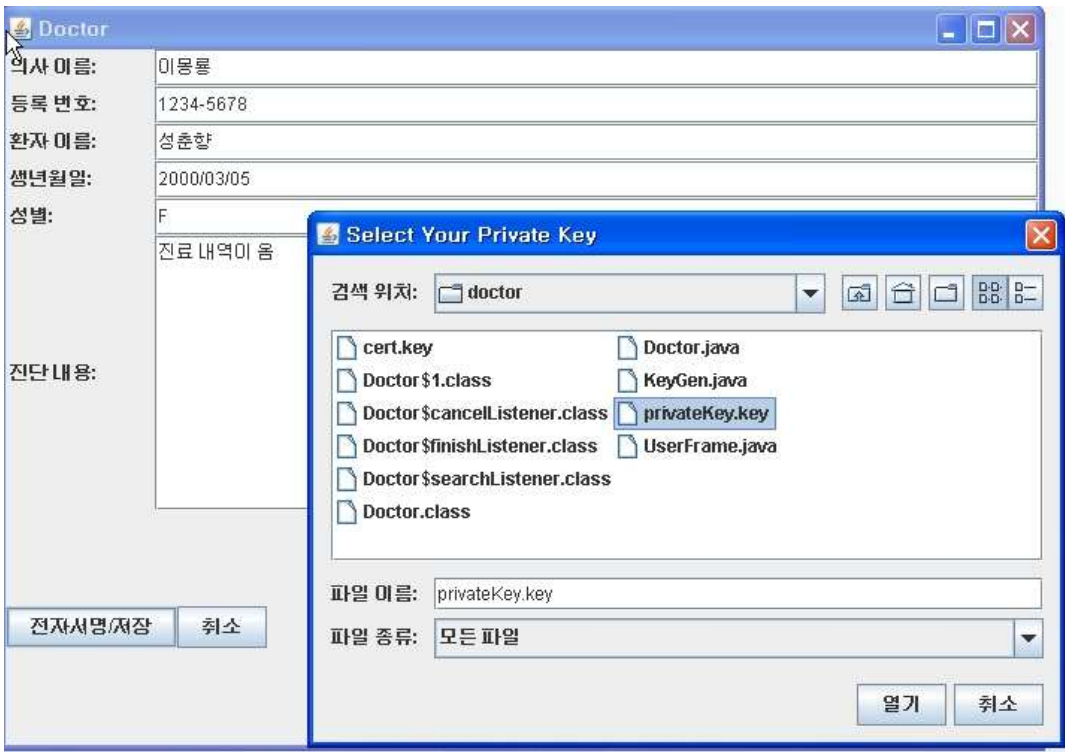
의료 분쟁이 발생한 경우, 의료기관은 자신이 보관하고 있는 의무기록이 변경되지 않았음을 증명할 수 있다.

논란이 발생한 의무기록이 c_i 이고, c_i 이후 최초로 공증받은 해쉬값이 h_m 이라고하자. $i \leq j \leq m$ 인 모든 의무기록에 대하여 $h_j=H(c_j \mid h_{j-1})$ 임을 확인하고 해당 전자서명이 해당 의무기록을 입력한 의료인의 올바른 전자서명이며, 공증받은 해쉬값 h_m 이 공증기관에 의하여 공증받았음을 보이면 된다. 공증 받은 시간 이후에는 변경이 있을 수 없다. 그리고 공증 받기 이전에 변경이 있는 경우라면 $i \leq j \leq m$ 인 의무기록 c_j 를 입력한 모든 의료인이 다시 전자서명을 하여야 가능하므로 가능성이 매우 낮다.

4. 프로토타입 설계

수행 분석을 위하여 3절에서 기술된 프로토콜을 바탕으로 프로토타입이 개발되었다. 프로토타입 시스템은 3 개의 서브시스템으로 구성된다. 의료인의 컴퓨터에서 의료인의 입력을 받아 전자서명하여 정보를 의료기관에 전송하는 Doctor 서브시스템, 의료기관으로부터 의무기록을 받아 저장하며 주기적으로 공증기관에게 의무기록에 대한 공증을 요청하여 공증정보를 저장하는 Hospital 서브시스템, 그리고 공증기관의 역할을 하는 Notary 서브시스템이 그들이다.

3개의 서브시스템 사이의 메시지 교환은 3.4절에서 기술된 것과 동일하다. 매번 의료인의 의무기록 입력이 완료되면 Doctor 서브시스템에서는 의료인의 전자서명이 수행되며 이 때 현재 의무기록 뿐만 아니라 이전 의무기록에 대한 해쉬값을 전달받아 현재 의무기록과 함께 해쉬한 후 이 해쉬값에 전자서명을 수행한다. 주기적으로 Hospital 서브시스템은 Notary 서브시스템에게 마지막으로 입력된 의무기록의 해쉬값 - 이 해쉬값은 해쉬체인에 의하여 이전 의무기록에 대한 정보도 함께 가지고 있음 - 을 Notary 서브



(그림 3) 의무기록 입력 및 전자서명 화면

시스템에게 전송하여 공증을 받아 공증 받은 결과를 저장한다. Notary 서브시스템은 공증 요청이 있는 경우 현재 시간을 첨부한 후 요청 내용에 전자서명을 하여 공증한 후 공증 결과를 반환한다.

Doctor 서브시스템은 의무기록을 의료기관에 저장하기위하여 매번 의무기록을 저장할 때 소켓프로그램을 이용하여 Hospital 서브시스템과 교신을 하였다. Hospital 서브시스템 또한 주기적으로 Notary 서브시스템과의 교신을 위하여 소켓 프로그램을 이용하였다. (그림 3)은 Doctor 서브시스템의 의무기록 입력/전자서명 화면을 보여준다.

Java를 이용하여 프로토타입이 작성 되었으며 암호화 알고리즘은 Java.Security 패키지에서 제공되는 알고리즘을 사용하였다.

해쉬는 SHA-1 해쉬 알고리즘을 사용하였다.

전자서명은 서명 대상을 SHA-1 해쉬를 이용하여 구한 해쉬값에 RSA 전자서명 알고리즘을 사용하였다.

수행 시간 측정을 위하여 프로토타입의 사용자인터페이스 부분의 사용자 입력을 컴퓨터가 자동 생성하도록 변환하여 측정하였다. 기존 기법의 시간 측정을 위하여서는 개발된 프로토타입의 연결해쉬와 전자공증 부분을 제거하고 전자서명 부분만 남겨서 사용하였다.

개발된 프로토타입은 의료인, 의료기관, 공증기관 모두 Intel Pentium 4 프로세서를 가지는 Windows XP 환경에서 수행되었다. 수행 시간을 측정한 결과는 <표 1>과 같다.

<표 1> 수행 시간

	기존기법	제안기법
수행시간 (초/1000회)	14	18

1000회의 자동입력된 의무기록을 처리하는데 걸린 시간은 기존의 전자서명만을 사용하는 경우 약 14초이며 이 논문에서 제안하는 경우 약 18초가 된다. 약 29%의 시간이 추가로 필요로 된다.

5. 분석 및 고찰

현재 사용되고 있는 종이의무기록의 경우 의료인이 서명한 의무기록을 의료기관에 보관한다. 이 경우 의료기관과 의료인이 공모하면 작성된 의무기록을 파기하고 새로 의무기록을 작성한 후 의료인이 서명함으로써 의무기록을 변경할 수 있는 여지가 있다.

전자의무기록의 경우 현재 사용되는 지침[7, 8]과 전자의무기록시스템[9, 10, 11] 또한 의료인이 전자서명한 전자의무기록을 의료기관에서 보관한다. 의료인의 전자서명을 의무기록에 첨부함으로써 의무기록 변경 방지 기능을 제공하는 것이다. 그러나 이 경우에도, 의료인과 의료기관이 공모하는 경우 의료기관에서 보관하고 있는 의무기록을 변경한 후 의료인이 다시 서명할 수 있으므로 의무기록의 신뢰성이 낮아진다. 또한 전자서명 후 전자의무기록을 변경하여도 이를 확인할 수 없으므로, 이는 전자서명이 있은 후 전자의무기록의 변경 여부를 확인할 수 있는 장비를 갖추어야 한다고 명시하고 있는 의료법 시행규칙[6]에도 위배된다.

본 논문에서 제안한 신뢰성 증진 기법은 의무기록이 생성된 후 변경될 수 있는 가능성을 획기적으로 낮추어준다. 제안된 기법을 사용하면, 의료인이 자신이 입력한 의무기록을 부인(변경)하는 경우 의무기관이 의료인의 의무기록 입력을 입증할 수 있다. 또한 환자가 의무기록 변경 가능성을 제기하는 경우에도 의무기록이 변경되지 않았음을 입증할 수 있다.

의료인이 자신이 입력한 의무기록을 의료기관의 동의 없이 변경하거나 입력 사실을 부인하는 것은 불가능하다. 의료인은 자신이 입력한 의무기록(c_i)과 바로 직전의 의무기록의 해쉬값(h_{i-1})을 연결한 값으로부터 해쉬값($h_i=H(c_i \ / \ h_{i-1})$)을 취한 후 이 해쉬값에 자신의 개인키($Priv_{ej}$)를 이용하여 전자서명($sign_{ej}(h_i)$)을 한 후 의료기관에 전송하며 의료기관은 해당 의무기록과 해쉬값 그리고 전자서명을 보관한다. 따라서 의료기관의 동의 없이 해당 의료인은 자신이 입력한 의무기록을 임의로 변경하거나 부인할 수 없다. 의료인의 개인키($Priv_{ej}$)를 가진 사람만이 전자서명을 수행할 수 있기 때문이다. 의무기관은 분쟁 발생 시, 의무기관에 보관 중인 해당 의무기록(c_i)과 그에 첨부된 의료인의 전자서명($sign_{ej}(h_i)$)이 해당 의료인의 개인키에 의하여 생성되었음을 보

임으로써 의료인이 해당 의무기록을 입력하였음을 증명할 수 있다.

의료인과 의료기관이 공모하여 의무기록을 변조하고자 하는 경우에도 의무기록 변경은 매우 어렵다. 의무기록 입력 후 공증 시점이 경과하면 의무기록 변경이 불가능하며 공증 시점 이전이라도 의무기록 변경은 매우 어렵다.

의료기관과 의료인은 공증기관으로부터 공증받은 이후에는 그 이전의 어떠한 의무기록에 대한 변경도 불가능하다. 즉 일정 시간 (해쉬값을 공증기관에 전송하는 시간) 이후에 의무기록을 변경하는 것은 불가능하다. 특정 시점(tS)에 공증받은 의무기록 번호가 m 이고 변경하고 싶은 의무기록의 번호가 i 인 경우 $i \leq m$ 이면, 의무기록 c_i 의 변경은 해쉬값 h_i 의 변경을 가져오며 이는 그 후속 의무기록의 모든 해쉬값(h_j, $where\ j \geq i$)의 변경이 필요하게 된다. 만약 후속 해쉬값 중 하나라도 변하지 않으면 그 경우, $h_k = H(c_k \mid h_{k-1})$을 만족하지 못하기 때문이다. 따라서 h_m 또한 변경되어야 한다. h_m 이 변경되면 공증기관으로부터 수신하여 보관하고 있는 공증 메시지의 공증기관 전자서명 ($sign_N(tS, h_m, sign_M(h_m))$) 또한 변경되어야 한다. 공증기관 전자서명은 공증기관에 의하여만 생성될 수 있으므로 의료기관은 새로운 공증 메시지를 생성할 수 없다. 따라서 공증이 이루어 진 후 공증 시점 이전의 의무기록을 변경하는 것은 불가능하다.

공증 시점 이전에 의료기관이 의무기록을 변경하는 것은 기능하기는 하지만 현실적으로 매우 어렵다. 마지막 공증이 일어난 이후에 입력된 i 번째 의무기록을 변경하면 그 의무기록 이후의 모든 의무기록의 해쉬값(h_j, $where\ i \leq j \leq m$)을 재계산하여야 하며 또한 이들 의무기록(c_j, $where\ i \leq j \leq m$)을 입력한 모든 의료인이 다시 전자서명을 수행하여야 한다. 종사하는 의료인의 수가 많은 경우 많은 시간이 필요할 뿐만 아니라 전자서명을 다시 수행하는 모든 의료인이 공모하여야 하므로 이는 현실적으로 불가능하다.

따라서 의료기관은 논란이 발생한 의무기록이 c_i 이고 c_i 이후 최초로 공증받은 해쉬값이 h_m 일 경우, $i \leq j \leq m$ 인 모든 의무기록에 대하여 $h_j=H(c_j \mid h_{j-1})$ 임을 보이고 그 의무기록들에 첨부된 전자서명이 해당 의무기록을 입력한 의료인의 올바른 전자서명임을 보이며, 공증받은 해쉬값 h_m 이 공증기관에 의하여 공증 받았음을 보임으로써 의무기록의 변경이 없음을 보일 수 있다.

제안된 기법으로 프로토타입을 작성하여 수행결과를 분석하였다. 기존의 전자의무기록시스템과 같이 의료인의 전자서명만을 의무기록에 첨부하는 경우 하나의 의무기록을 처리하는데 14/1000초가 필요하였으며 본 논문에서 제안된 기법을 사용하는 경우 하나의 의무기록을 처리하는데 18/1000 초가 필요하였다. 기존의 전자서명만을 사용하는 전자의무기록 기법에 비교하여 제안된 기법은 약 29%의 시간이 추가로 필요로 된다. 그러나 의료인이 입력하는 시간을 고려하면 무시할 수 있는 시간이 된다. 즉 한 건의 의무기록을 처리하는데 제안 기법은 약 18/1000 초가 소요되므로 의료인의 입력 시간과 비교하면 무시될 수 있다.

이 논문에서 제안된 기법을 사용하는 경우 비용의 증가는 크지 않다. 의료기관의 경우 매 의무기록 저장 시 해쉬값 계산을 하는 시간이 추가되나 해쉬 계산은 매우 빠르므로 추가되는 비용은 무시할 수 있다. 또한 일정 시간마다 의료기관의 개인키를 이용하여 전자서명하고 그 결과를 공증기관에 전송하고 공증된 값을 수신하는 비용이 추가되나 송수신 정보가 매우 작고 일정 시간마다 한 번씩 수행하므로 추가되는 비용은 무시할 수 있는 정도이다.

이 기법을 사용하기 위해서는 공증기관이 필요하다. 공증기관은 현재 존재하는 공적 기관인 정부기관 또는 공인인증기관 등이 수행할 수 있다. 각 공증기관은 자신이 관할하는 모든 의료기관으로부터 수신한 해쉬값과 전자서명을 확인하고 이에 다시 전자서명하여 해당 의료기관으로 송신하여야 한다. 그러나 공증기관 또한 일정 시간마다 다른 처리 없이 전자서명 확인과 전자서명 생성만 하므로 비용의 부담이 과도하게 증가하지는 않을 수 있다.

6. 결론

의무기록은 의료기관에서 보관하는 환자의 의

료정보에 관한 기록으로 매우 중요한 기록이다. 의료기관 종사자에 의하여 서명된 의무기록은 해당 의료기관에서만 보관되므로 서명 이후에 의료인과 의료기관의 공모에 의하여 의무기록이 변경될 수 있는 여지를 남겨놓고 있다. 종이의무기록과 전자의무기록 모두 이에 해당한다. 이는 의료분쟁이 발생하는 경우 중요한 증거 가운데 하나인 의무기록에 대한 신뢰성에 심각한 영향을 주며 의무기록 변경에 대한 논쟁의 불씨를 제공하게 된다. 또한

컴퓨터의 발달과 함께 종이의무기록이 컴퓨터에 기록하고 저장하는 전자의무기록으로 바뀌고 있다. 전자의무기록을 사용하는 경우 암호학적 기법을 이용하여 의무기록의 신뢰성을 높일 수 있다.

본 논문에서는 전자의무기록의 변경을 어렵게 하여 의무기록의 신뢰성을 높일 수 있는 기법을 제안하였다. 제안된 기법은 의료인과 의료기관의 공모하는 경우에도 의무기록을 변경하기가 매우 어려우며 일정 시간 후에는 의무기록을 절대로 변경할 수 없다. 제안 된 기법은 현재의 전자의무기록 외에 매우 적은 추가 비용으로 의무기록의 신뢰성을 향상시킬 수 있으며 불필요한 의무기록의 변경에 대한 논쟁을 피할 수 있도록 하며 또한 전자서명 후 전자의무기록의 변경 여부를 확인할 수 있는 장비가 필요하다고 명시한 의료법 시행규칙[6] 또한 준수한다.

보건산업진흥원에서 개발한 전자의무기록에 대한 공인전자서명 적용 지침에서 전자의무기록의 법적 보호를 위하여 전자의무기록에 공인전자서명 첨부하라고 기재하고 있으나 이 경우 전자서명이 있은 후 전자의무기록의 변경 여부를 확인할 수 있는 장비를 갖추어야 한다고 명시하고 있는 의료법 시행규칙[6]에 적합하지 않으므로 전자서명 후 전자의무기록을 변경할 수 없도록 개정될 필요가 있다.

참 고 문 헌

[1] 2005년도 의료 피해구제 업무분석 결과, 한국소비자원, 2006.

[2] 전영주, “의료법상 의료정보 보호방안 - 의무기록 보호를 중심으로”, 법학연구, 28, pp. 465-483, 2007.

[3] 의료법, 법률 제 9923호, 2010.

[4] 김경호, “전자의무기록(EMR)을 활용한 원무관리 개선“ 법과 정책연구, 6(1), pp. 95-115, 2006.

[5] 전자서명법, 법률 제9208호, 2008.

[6] 의료법 시행규칙, 보건복지부령 제 1호, 2010.

[7] 전자의무기록에 대한 공인전자서명 적용 지침, 정책-의료정보-2004-57, 한국보건산업진흥원, 2004.

[8] 신용원, 박정선, “전자의무기록에 대한 공인전자서명 적용 지침 개발”, 한국콘텐츠학회논문지, 5(6), pp. 120 - 128, 2005.

[9] 하규섭, EMR 개발의 실제-분당 서울대병원 EMR 구축과 활용, 분당서울대병원 의료정보과, 2004.

[10] 전자의무기록 시스템 - bitnix EMR, http://www.bit.kr/image/02_business/emr/emr.pdf.

[11] 전자의무기록 시스템 소개 (FK-EMR), 한국 후지쯔 주식회사, 2007.

[12] W. Stallings, Cryptography and Network Security - Principles and Practices, 4th Edition, Pearson Education, 2006.

[13] R. L. Rivest, "The MD5 message-digest algorithm", RFC 1321, 1992.

[14] "Secure Hash Standard", FIPS 180-1, NIST, 1995.

[15] R. L. Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Vol 21, pp. 120-126, 1978.

[16] "Digital Signature Standard", FIPS 186, NIST, 1994.

[17] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.

주 한 규

1988년 : 한림대학교 전자계산학과 졸업 (이학사)

1994년 : 아리조나 주립대 컴퓨터공학과 졸업 (공학석사)

1998년 : 아리조나 주립대 컴퓨터공학과 졸업 (공학박사)

1999년～2000년: 한국전자통신연구원 선임연구원

2000년～현 재: 한림대학교 컴퓨터공학과 부교수

관심분야 : 소프트웨어공학, 정보보호