키등급을 이용한 병원정보시스템에서의 개인정보 보안

배 석 찬
군산대학교 컴퓨터정보과학과
e-mail:scbae@kunsan.ac.kr

Personal Information Security in Hospital Information Systems Using Degree of Key

Seok-Chan Bae
Dept. of Computer Information Science, Kunsan Nat'l Univ.

요 약

병원에서 개인정보유출이 심각하여 병원 데이터베이스 내의 환자 차트와 전자처방전의 유출과 오용에 대비하여야 한다. 최근에는 의료 정보시스템이 통합, 발전하고 있다. 이러한 시스템을 구축, 사용 그리고 공유함으로써 환자를 잘 돌봐주고, 환자의 개인 사생활이 침해받지 않는 것이 중요하다. 그러나 여러 가지 유형의 개인정보 침해 가능성이 존재하기 때문에 이에 대비한 개인정보 보호가 필요하다. 그래서 본 논문에서는 사용자 그룹이 접근하고자 하는 서버에서의 환자 의무기록 사항에 대해 보안정책을 고려하여 자동적으로 키 등급을 비교하여 등급 생성 및 저장한다. 접근하고자 하는 서버의 자료와 등급을 비교하여 더 높은 키등급을 소유하고 있는 사용자가 서버에 있는 자료를 열람 및 기타 연산이 가능하도록 하였다.

1. 서론

최근 인터넷이 실시간 언제 어디서나 사용하게됨에 따라 공공기관 뿐만아니라 병원에서도 인터넷과 클라이언트/서버 환경이 구축되어 진료 예약과 진료결과를 집이나 휴대폰으로 손쉽게 알 수 있다. 이처럼 편리하게 됨에 따라 잘못된 생각으로 개인정보 유출 또한 유출된 정보의 유용이 우려된다.

1999년 1월 29일 개정한 법률 5715호인 개인정보보호법, 공공기관의 컴퓨터에 의해 처리되는 개인정보를 보호하기 위해 그 취급에 관해 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모하고 국민의 권익을 보호할 목적으로 제정한 법(1994. 1. 7, 법률 제4743호)으로 개인 사생활의 비밀을 보호하고 사적 권익의 침해를 방지하고 있다[1].

또한 2005년 3월 31일 개정한 법률 7427호인 국가인권위원회법을 통하여 모든 개인이 가지는 불가침의 기본적 인권을 보호하고 인권의 보호와 향상을 위한 업무를 수행하기 위하여 국가인권위원회를 두었다(2001. 5. 24, 법률 제6481호)[1].

그러나 주민등록번호 및 기타 개인정보의 노출로 인권 침해 및 범죄의 활용 가능성이 더욱 증가하고 있다.

의료기관 내에서 병원 정보 시스템이 통합하여 발전하고 있다. 이 시스템을 구축, 사용 그리고 공유함으로써 환자를 잘 돌봐주고, 환자의 개인 사생활이 침해받지 않는 것이 중요하다. 또한 시스템의 기밀성과 무결성을 보호함과 동시에 허가된 자만에게 시스템을 이용하도록 보장받는 것이 요구사항이다. 변화되어가는 환경에서 중요한 것은 모든 대량의 자료가 전자적으로 되고 있는데, 정보의 무결성이 유지되면서 데이터베이스 내에 저장 및 관리되어져야 한다[2].

개인병원, 중·대형 병원이나 약국에서 개인 신용정보 유출에 따른 개인 프라이버시 침해와 사적인 거래의 문제가 있고, 이에 대한 개인 병력을 해킹, 유출, 부적절하게 이용하고, 개인 생활을 침해할 가능성이 있다.

개인병원이나 대형병원의 단말기를 통해 허가권자가 아니더라도 환자의 이름 입력을 통해서 개인정보 유출이 손쉽게 이루어질 수 있어 이에 대비한 병원 정보시스템에서 보안 연구가 필요하다.

그래서 본 논문에서는 키등급을 이용한 병원정보 시스템에서 개인정보의 보안정책을 연구하였다.

본 논문의 구성은 다음과 같다. 2장에서는 데이터베이스 보안과 개인정보 보호의 필요성에 대해서 언급하였다. 3장에서는 접근제어 정책과 전체의 시스템 구조, 의무기록 절차에 대해서 기술하였다. 4장에서는 결론 및 앞으로의 연구방향에 대해서 기술하였다.

2. 데이터베이스 보안과 개인정보 보호의 필요성

2.1 데이터베이스 보안

데이터베이스에서 정보 보안은 정보의 부적절한 유출방지/탐지/제지를 의미하는 비밀성(Secrecy), 정보의 부적절한 수정을 방지/탐지/제지를 의미하는 무결성(Integrity), 시스템이 제공하는 서비스 접근에 대한 부적절한 거부를 방지/탐지/제지하는 가용성(Availability) 등 세가지 특성을 포함하고 있다[3].

가능한 위협으로부터 데이터베이스를 보호하는 것은 우연, 고의적, 비권한 열람 및 갱신으로부터 저장자료를 보호하는 것을 말한다[4].

<표 1> 현재의 개인정보 침해 유형

개인정보 침해 유형	현 재
부적절한 접근과 수집	정보주체의 동의없는 개인정보의 수집
부적절한 분석	부적절하게 수집된 정보의 분석, 동의없는 사적 정보의 분석
부적절한 모니터링	동의없는 개인 인터넷활동의 모니터링
부적절한 개인정보유통	개인정보를 제3자에게 양도하는 불법적 거래
원하지 않은 영업행위	동의없는 상품광고, 광고성정보전송행위
부적절한 저장	정보수집 목적 달성후 개인정보를 파기하지 않는 행위

일반적인 개인 정보로는 이름, 주민등록번호, 주소, 전화번호, 성별, 휴대폰번호 등이 있고, 의료정보에는 환자번호, 등록날짜, 가족병력기록, 과거의료기록, 정신질환기록, 등 각종 의료정보가 있다. 또 다른 신체정보로는 지문, 홍채, 손혈관인식, DNA, 신장, 가슴둘레, 몸무게 등이 있다. 이와같이 개인의 신상 및 이에 관련된 정보가 대부분이다.

개인정보를 이용하여 인터넷, 각종 마케팅 행사, 다양한 사이트나 기관에 등록되고, 저장된 개인정보, 설문조사 등의 방법으로 각 개인이 원하든 원하지 않든 각종 저장매체에 기록되고 유통될 수 있다.
이와같은 정보가 <표 1>과 같이 침해가능성이 있다[5].

개인정보 침해 유형을 살펴보면, 첫째로 부적절한 접근과 수집으로 정보주체의 동의 없이 개인정보를 수집, 수집시 고지 또는 명시의무를 이행하지 않는 것이 이에 속한다. 둘째로, 부적절한 모니터링이다.

인터넷 마케팅업체들은 쿠기나 접속한 개인의 클릭 스트림 조사 방법을 사용해서 소비자들이 어느 사이트를 접속해 얼마나 머무르고 어떤 거래를 하는지를 알아낸다. 셋째, 부적절한 분석이다. 소비자들이나 노동자들에게 알리지 않고, 그들의 사적인 정보를 분석하는 행위를 말한다. 부적절하게 접근되고 수집된 정보와 모니터링 정보가 분석되면 이는 부적절한 분석이 된다. 넷째, 부적절한 개인정보의 유통이다. 대부분의 개인 정보 유출의 형태이기도 하다. 고객에게 알리지 않고 고객의 개인정보를 다른 기업들에게 넘겨주는 행위가 이에 속한다. 다섯째, 원하지 않은 영업행위이다. 주로 인터넷 사용자의 동의나 허가없이 상품광고 메일을 보내는 행위를 말한다. 여섯째, 부적절한 저장이다. 개인정보를 안전하지 못한 방식으로 보관하여 저장된 정보의 신뢰성을 떨어뜨리고 정보접근에 대한 인증을 수행하지 못하는 행위를 말한다. 데이터베이스 시스템 관리를 잘못하여 개인사용자가 다른 사용자의 정보를 훔쳐볼 수 있다.

2.2 개인정보 보호의 필요성

현재 우리가 살고 있는 실생활 내에서 개인정보 침해 유형을 살펴보면, 여러 가지 유형의 개인정보 침해 가능성이 존재하기 때문에 이에 대비한 개인정보 보호가 필요하다.

의료기관의 개인 정보 유출에 대한 대책 마련도 미흡하지만 외부의 해킹에 의한 개인 정보 유출보다 병원 내부근무자나 의료 정보 업체 직원들에 의한 정보 유출이 더 심각하다. 사례에 따르면 병원사무장이 전자처방전을 통해 환자 4천명의 개인정보를 빼내 다른 사이트를 개설해 운영하다 적발한 경우도

있다. 또한 병원 직원뿐만 아니라 의료정보 업체 직원들에 의한 정보 유출도 심각하다. 병의원 진료차트 관리 프로그램을 제작·공급하는 업체 대표 등 직원이 국내 50여개 병의원으로부터 230여만 건에 달하는 환자진료정보를 외부로 유출한 사례도 있다. 그리고 프로그램 업데이트 및 유지보수를 위해 필요하다는 이유로 병원들로부터 환자의 진료정보가 포함된 수십만건의 자료를 자연스럽게 넘겨받았다[6].

이처럼 시스템 유지보수 관리 업체에서 병원 데이터베이스에 기록된 환자 및 개인정보를 언제든지 볼 수 있고, 또한 전자처방전 전달시스템에 의해서도 개인정보 유출 가능성이 있다. 그래서 병원정보시스템에서의 개인정보 유출에 대비한 연구가 필요하다.

3. 접근제어 정책과 시스템 구조

강제적 접근 제어 정책은 Bell과 Lapadula가 설계한 모델에 기반하고 있다[7]. 이는 시스템에 있는 주체(Subject)와 객체(Object)의 분류 등급에 따라 접근을 통제한다. 주체와 객체의 보안 등급은 4개의 원소 TopSecret(TS), Secret(S), Confidential(C), Unclassification(U)으로 되어 있으며, TS > S > C > U의 관계가 있다. 이 정책은 자신의 접근 등급 이하인 객체만을 판독가능하며 주체는 자신의 접근 등급 이상인 객체만을 기록 가능하다. 그래서 시스템 자료와 사용자가 등급화된 환경에서 강한보호가 필요한 대량의 정보에 적용되며, 데이터 침입을 보호하도록 설계되었다. 그러나 접근 권한 전달에 대하여 할당된 권한은 변경할 수 없으며, 권한 관리자만이 수정 가능하다[8].

3.1 보안정책과 사용자 정의

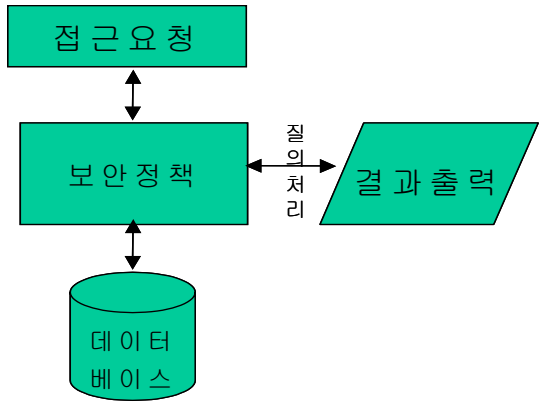
(보안정책 1) 키등급 K_i는 등급이 낮은 키그룹 K_j($K_i \geq K_j$)에 대하여 Read, Insert, Update, Delelte 가능하다.

(보안정책 2) 키등급 $K_i \in R^c$이고, R^c에 속할 경우 K_i는 Read, Insert, Update, Delete 가능하다.

(사용자 정의) 사용자는 정보 접근의 주체로서 데이타베이스의 사용자 또는 사용자 그룹을 의미한다. 병원 내에서는 의사, 간호사, 검사담당자, 영양사, 약사, 일반직원, 환자, 서버 담당자 등으로 구분할 수 있다.

사용자 1은 약사, 영양사로서 약제와 영양 조언에 필요한 환자 의무기록만 열람 가능. 사용자 2는 검사담당자로서 해당일자 검사환자의 검사결과를 열람 및 추가 가능. 사용자 3은 의사로서 병원 내 환자의 의무기록 열람, 추가, 갱신, 삭제 가능. 간호사는 해당 병동 내 환자의 의무기록 열람, 간호기록 작성 가능. 일반직원은 의무기록 서버에 접근 불가. 환자와 보호자는 환자 본인의 의무기록을 종이나 CD 등으로 복사하여 열람 가능. 서버 담당자는 서버를 관리한다.

3.2 시스템 구조



(그림 1) 시스템 구조

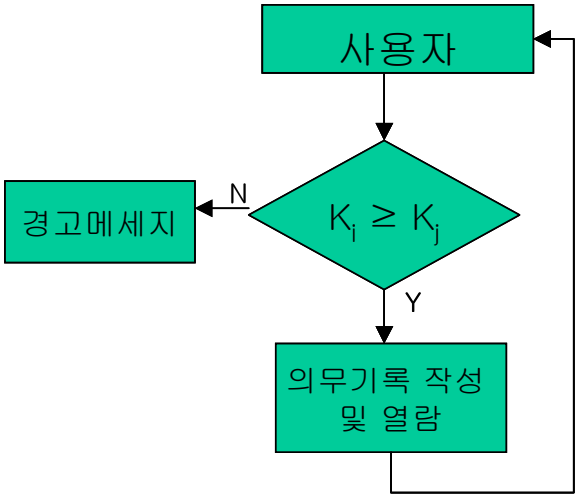
환자가 병원을 방문하여 접수창구에 접수, 의무기록 기초사항을 입력 및 조회하여, 기존 환자이면 환자번호나 이름, 주민등록번호를 검색, 챠트 탐색한다. 환자가 진료과에 대기함으로써 의사의 진료, 검사, 처방이 가능하다.

접수시 사용자 그룹이 접근하고자 하는 서버에서의 환자의무기록 사항에 대해 보안정책을 고려하여 자동적으로 키 등급을 비교하여 등급 생성 및 저장한다.

그림 1은 전체 시스템의 구조를 보여주고 있다. 사용자가 서버에 있는 데이터베이스에 접근을 요청하면 보안정책이 질의문을 추출하여 질의를 한다. 접근요청이 가능하면 서버에 있는 자료와 등급과 비교하여 더 높은 키등급을 소유하고 있는 사용자가 서버에 있는 자료를 열람 및 기타 연산이 가능하다.

3.3 의무기록 절차

사용자 K_i가 환자의 의무기록을 접근하고자 할 경우, 그림 2의 사용자 접근 절차 모듈의 3.1에서 언급한 보안정책 1과 2에 따라 사용자 속한 그룹의 키 등급을 비교하고, 역할을 식별하여 권한이 있는지 검사한다. 권한이 있어 접근이 가능하면 접근이 허용되고, 권한이 없으면 경고 메세지와 함께 접근을 거부한다. 접근이 가능해도 개인정보 유출 방지를 위하여 담당 의사외에는 모든 사용자에게 보여지는 전자의무기록과 환자나 보호자



(그림 2) 사용자 접근 절차

에게 주어지는 전자처방전에서 환자 본인 주민등록번호 뒤의 7자리는 '*******'로 채워지고, 또한 환자번호도 앞자리 4자리를 '****'로 채워지고, 질병분류기호도 '****'로 채워지고, 처방의약품의 명칭과 1회 투여량, 1일 투여횟수, 총투약일수, 총량, 용법 등은 보여지도록 하여 약사가 처방전에 표시되어 있는 약품에 대해서는 정확히 인지하도록 한다.

4. 결 론

최근 병원정보시스템에서 환자 개인정보 유출이 가능성이 있어 병원 내의 환자 차트와 전자처방전의 유출과 오용에 대비한 보안 연구가 필요하다.

그래서 본 논문에서는 비인가권자가 자료를 열람 및 갱신하고자 할때 키등급을 이용하여 병원정보시스템내에서 개인정보 보안 정책을 연구하였다.

이처럼 병원의 서버에 전자적으로 기록 저장되어 있는 환자의무기록을 열람할 수 있는 권한을 비교, 검사한 후 접근 가능하도록 하고, 환자나 보호자 개인에게 주어지는 처방전을 약사에게 전달할 경우 조제시 필요한 내용만으로 열람 조제 가능하도록 조치함으로써 개인정보보호법에 의거하여 개인정보 유출을 미연에 방지하고자 하였다.

앞으로의 연구방향은 인트라넷보다는 인터넷의 발달로 다른 병원이나 다른 지역병원과 연계하여 환자가 살고 있는 지역 가까운 병원에서도 대형병원과 동일한 진료가 가능하게 하는 분산환경에서도 정보보호를 강화할 수 있는 보안 정책에 대한 연구가 필요하겠다.

참고문헌

[1] http://search.assembly.go.kr:8080/law/

[2] E.Smith, J.H.P.Eloff, "Security in health-care information systems-current trends,"Int. Jour. of Medical Informatics, Vol. 54, pp.39-54, 1999.

[3] D.Russell, G.T.Gangemi, Computer Security Basics, O'reill & Associates, 1989.

[4] E.B.Fernandez, R.C Summers & C. Wood, Database Security and Integrity, Addison-Wesley, 1981.

[5] http://www.dbguide.net/

[6] http://www.plusclinic.com/

[7] R.Lindgreen and I.Herschberg,"On the Validity of the Bell-LaPadula Model," Computer & Society, Vol.13, pp. 317-338, 1994.

[8] S.Castano, M.Fugini, G. Martella & P. Samarti, Database Security, Addison-Wesley, 1994.