대한의료정보학회지 제10권 제3호
J Kor Soc Med Informatics 2004;10(3):269-278

다중 환자 정보 저장소에 대한 웹기반 보안 접근

최 준, 김남현, 유선국[1]

연세대학교 의과대학 의공학교실, 연세대학교 의과대학 의공학교실 & 이동형 응급의료정보시스템 개발센터[1]

Web-based Secure Access from Multiple Patient Reservoirs

Jun Choe, N. H. Kim, Sun K Yoo[1]

Dept. of Medical Engineering, College of Medicine, Yonsei Univ.;
Dept. of Medical Engineering, College of Medicine, Yonsei Univ., Center for Emergency Medical Informatics[1]

Abstract

Objective: For the ubiquity of medical service, when user who has proper authority want to access medical data, user accessability should be assured. And the security of the disclosed medical data is important. This paper presents single user access interface on multiple patient reservoirs and elaborate access control using the Role-Based Access Control(RBAC) system. **Methods:** Proposed system consists of 4-tier architecture that is client application, Access Control Central(ACC) agent, Local Access Control(LAC) agent and Hospital Information Systems(HIS). User requests medical data with client application. ACC notarizes user identity and controls access of user request and selectively encrypts medical data. LAC charges data conversion for communication between ACC and HIS. HIS has repositories of medical datum. System provides security service with digital certificate, X.509v3, of user. **Results:** User requests medical data of several HIS approaching single ACC not by each HIS. Through conversion process of LAC, data that is described XML and is used for communication inter system enables information exchange with single common data format that is independent to several HIS. **Conclusion:** In the proposed system, user accesses medical datum of several HIS regardless of location and has consistent access interface. And using independent format against each HIS makes easy information exchange between several HIS. Transferred data maintains security about significant datum by selective encryption and increases encryption efficiency. Unified access control about multiple patient reservoirs that are scattered in other places provides unified and precise diagnosis of patient information. And it functions the portal of collaborate treatment in inter-HIS. ***(Journal of Korean Society of Medical Informatics 10-3,269-278, 2004)***

Key words: Hospital Information Systems, Accessibility of Health Services, Data Security, Integrated Health Care Systems

논문투고일: 2004년 7월 14일, **심사완료일**: 2004년 9월 3일
교신저자: 유선국. 서울특별시 서대문구 신촌동 134 연세대학교 의과대학 의학공학교실(120-752)
전화: 02-361-5403 **Fax**: 02-392-4358 **E-mail**: sunkyoo@yumc.yonsei.ac.kr
*본 연구는 2003년도 보건복지부지정 특정센터연구지원 연구개발 사업 연구비에 의하여 연구되었음(과제번호: 02-PJ3-PG6-EV08-0001).

I. 서 론

정보통신기술의 발달에 따른 중요정보에 대한 데이터 침해사례는 해마다 증가추세에 있다. 의료분야에서도, 의료 정보보호에 대한 연구와 관심이 계속 커지고 있다. 'Anywhere, anytime, anything'의 유비쿼토스 환경을 목표로 산업계와 학술계 모두 정진하고 있으며, 웹은 실생활의 유비쿼토스를 위한 좋은 장이 되고 있다. 웹을 통한 의료서비스의 수준이 아직은 미약하지만 종이 없는 디지털 병원 및 재택의료 서비스 등 다양한 시도는 곧 웹을 통한 광범위한 의료서비스가 시작될 것임을 예고한다[1)2)]. 재택의료 서비스에서, 환자는 웹을 통해 여러 병원정보시스템에 접근하여 자신의 진료정보를 살펴볼 수 있어야 한다. 환자는 다양한 병원을 옮겨 다니며, 각 환자의 데이터들은 각 병원에 흩어져서 저장이 된다. 여러 곳에 분산된 환자데이터에 대한 통합적인 정보 수집을 통해 환자에 대한 더욱 질 좋은 서비스를 기대할 수 있다. 또한 병원 간 정보공유는 다양한 의료시술에 대한 간접적 경험의 폭을 넓혀 병원 서비스의 질을 향상시킨다. 이와 더불어 여러 악의적인 공격으로부터 병원정보시스템의 안정적인 접근제어와 공용 망을 통한 데이터 전송에 대한 의료보안은 중요한 이슈가 되고 있다. 이를 위해 병원정보시스템의 접근제어를 다루는 보안모델과 여러 병원정보시스템 간의 정보교환을 위한 구조를 제안하고 있다[3-7]. 이들 모델에서는 사용자는 특정 시스템에 종속적이다. 또한 병원정보시스템 간의 정보교환에 있어 1:m의 신뢰 관계를 통해 여러 병원정보시스템들 간의 정보교환에 있어 추가/삭제에서 유연하지 못한 단점이 있다. 기존 병원정보시스템들은 이미 구축된 상이한 접근제어시스템을 갖추고 있다. 각 병원정보시스템에 독립된, 여러 곳에 분산 저장된 환자 정보를 접근할 수 있는 포탈로서의 시스템이 고려되어야 한다. 시스템 접근제어를 하기위해 사용자에게 접근제어리스트(ACLs)를 할당하는 기존의 사용자기반 접근제어 시스템은 유연성과 확장성, 관리운용에 있어 단점을 갖는다. 이를 보완하고자 제시된, Role-Based Access Control(RBAC) 시스템은 각 사용자들의 공통되는 접근제어리스트를 역할로 묶고 역할들을 사용자에게 할당한다[7-9]. 시스템에 대한 접근제어리스트와 사용자를 서로 분리시켜 정책 관리자의 접근제어 관리를 단순화시킨다. 또한 단순한 접근리스트가 아닌 의미 있는 역할을 통한 접근제어를 함으로써 관리를 더욱 정교하게 한다. 본 논문에서는 허가된 사용자가 여러 병원정보시스템들을 장소 및 플랫폼에 제약을 받지 않고 접근할 수 있는 시스템 구조를 제안한다. 여러 병원정보시스템과의 정보공유를 위해서 각 병원정보시스템은 서로의 접근권한을 허가하는 상호 신뢰관계여야 한다. 이 경우 새로운 병원정보시스템이 기존 병원정보시스템들과 신뢰관계를 맺기 위한 트랜잭션들은 기하급수적으로 증가한다. 이런 제약사항을 해결하기 위해, 병원정보시스템은 다른 병원정보시스템들과의 신뢰관계를 갖는 중간 에이전트와 신뢰관계를 형성한다. 이 후 각 병원정보시스템은 에이전트를 통해 다른 병원정보시스템들과 정보공유를 함으로써 신뢰관계를 맺는 트랜잭션의 수를 선형적으로 만든다. 공통 데이터 포맷을 갖지 않는 시

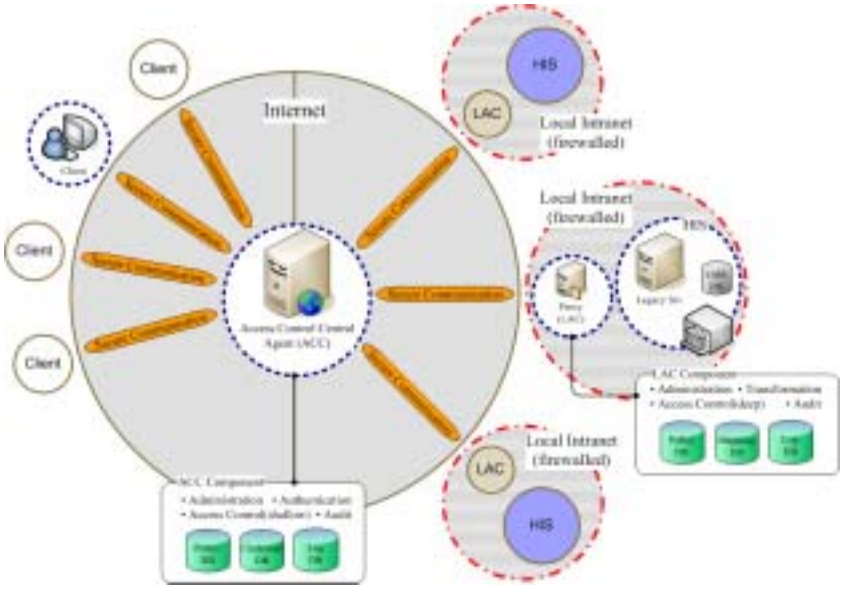

Figure 1. System architecture

스템간의 정보공유는 정보변환을 위해 기하급수적인 비용문제를 만든다. 이를 해결하기 위해 각 시스템의 상이한 형식의 데이터를 공통 포맷으로 변환하여 정보공유를 함으로써 시스템간의 지수적인 정보변환 비용문제를 선형적으로 만든다. 또한 병원정보시스템 간 환자데이터 공유 시 민감한 또는 기밀데이터에 대한 보호를 위해 월드와이드웹 컨소시엄(W3C)에서 제안된 XML Security 기술을 이용한다. XML Security는 XML Signature와 XML Encryption로 구성되며, 이를 이용하여 선택적 암호화와 디지털 서명을 함으로써 효과적 데이터 보호를 한다[10-13].

II. 시스템 요구사항

1. 통합된 접근제어

웹기반 다중 환자 정보 저장소에 대한 통합된 접근제어를 위해 시스템은 상호운용성(Interoperability), 접근성(Accessibility), 확장성(Scalability) 및 유연성(Flexibility)을 만족하여야 한다. 사용자는 중앙접근제어 에이전트를 통해 여러 상이한 플랫폼의 병원정보시스템에 접근한다. 각 HIS는 객체 타입(진단서, PACS 영상, 처방서 등 구조적 분류)별 개념적으로 동일한 환자데이터 포맷을 가지며 단일 포맷을 갖는 데이터로 변환이 가능하다고 가정한다. 시스템은 데이터 전송 간 XML로 표기된 공통 데이터 포맷을 사용한다. 이를 통해 전송 데이터는 각 병원정보시스템의 플랫폼에 독립적이 된다. 사용자는 플랫폼에 상관없이 각 병원정보시스템을 동일한 접근 인터페이스를 통해 이용하며, 시스템은 상호운용성을 만족한다. 시스템은 장소에 상관없이 항상 병원정보시스템의 접근성을 보장한다. 각 병원정보시스템들은 서로 배타, 독립적이며 오직 접근제어 에이전트를 통해 접근이 가능하다. 접근제어 에이전트를 통한 중앙 관리는 신규 병원정보시스템의 추가, 삭제를 단순화하며, 확장성을 보장한다. 시스템을 구성하는 컴포넌트들 간은 서로 독립적(종속성 제거)이어서 개별 컴포넌트의 변경이 다른 컴포넌트에 영향을 미치지 않는다. 즉 개별 컴포넌트의 변경에 유연한 구조를 통해 유연성을 만족한다. 접근제어를 위한 정책관리는 병원정보시스템을 이용하는 기존 내부사용자와 그렇지 않은 외부사용자로 구분된 이중정책을 통해 이뤄진다.

2. 보안 사항

시스템은 네트워크 전송, 사용자의 데이터 유출 등 데이터의 보호를 위해 암호화와 전자서명을 통한 기밀성, 무결성 등 보안 서비스를 제공한다. 사용자의 공개키 기반 공인인증서(X.509v3)를 통해 사용자 인증을 한다[14]. 보호가 필요한 민감/기밀 데이터에 대한 선택적 암호화를 통해 기밀성을 제공한다. 민감 또는 기밀이 요구되는 중요 데이터에 대한 각 병원정보시스템의 정의가 일치할 때, 시스템은 데이터의 객체 타입에 따른 보호가 필요한 부분에 대한 세밀한 정보를 갖는 메타데이터(암호화 트리)를 갖는다. 전송되는 데이터에 데이터의 전자서명을 첨부하여 무결성을 보장한다. 기존 병원정보시스템은 자체 방화벽 등에 의해 외부로부터 안전하게 보호되어 있다고 가정한다. 사용자와 병원정보시스템간의 모든 트랜잭션은 로그 정보를 남겨 감사를 지원한다.

III. 제안된 시스템 구조

제안된 시스템은 클라이언트 애플리케이션, 중앙접근제어 에이전트(ACC), 지역접근제어 에이전트(LAC), 기존 병원정보시스템(HIS)으로 이뤄진 4-티어 구조(Fig. 2)이다.

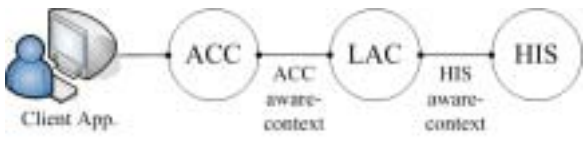

Figure 2. Proposed system architecture(4-tier)

시스템의 대략적인 동작 프로세스는 다음과 같다. 사용자는 클라이언트 애플리케이션을 통해 ACC에 접근한다. ACC는 사용자를 인증하며, 데이터의 선택적 암호화를 위한 세션키를 전송한다. 사용자의 요청은 ACC에 의해 낮은 수준의 요청 적합성(U-R 관계) 검증 후 요청 데이터가 있는 해당 HIS의 LAC으로

요청을 전달한다. 전달된 요청은 LAC에 의해 요청 적합성(U-R 관계)을 재검증한다. 승인된 요청에 대해 HIS가 이해하는 요청 포맷으로 변환한 후 요청을 전달한다. HIS는 전달된 요청에 대해 사용자에게 인가된 권한인지를 (R-P 관계) 검증 후, 승인된 요청에 대해 결과 데이터를 LAC로 반환한다. LAC는 반환된 데이터에 대해 ACC가 이해하는 데이터 공통 포맷으로 변환하여 전달하며, ACC는 받은 데이터의 객체 타입에 따른 민감/기밀 정보에 따라 세션키를 이용한 선택적 암호화를 하여 사용자에게 전달한다. 사용자와 ACC 간은 세션키를 통한 전송 간 보안을 제공하며, ACC와 LAC는 공개키 기반 공인 인증서를 이용한 암호화를 통해 기밀성을 유지한다. HIS와 LAC 간의 전송은 병원 내부의 방화벽에 의해 보안 유지되어 있다고 가정한다. 모든 요청, 응답에 대한 트랜잭션은 로그정보를 남겨 감사를 지원한다. 시스템의 각 구성요소별 역할은 다음과 같다.

1. 클라이언트 애플리케이션

클라이언트 애플리케이션은 사용자가 접근제어 에이전트를 통해 다중 병원정보시스템에 접근 할 수 있는 단말 노드에 해당한다. 사용자의 인증(로그인) 및 접근제어 에이전트 간의 암호화 된 데이터의 복호화와 사용자의 전자 서명 첨가, 전송 데이터의 무결성 검증 및 편리한 사용자 인터페이스를 제공한다. 모든 사용자는 고유 인증서(X.509v3)를 갖으며, 인증서 기반 사용자의 인증을 한다.

2. 중앙접근제어 에이전트 (ACC; Access Control Central Agent)

ACC는 사용자의 인증(User authentication), 감사(Audit) 및 HIS의 EMR 데이터 요청에 대한 낮은 수준의 접근제어 유효성(User-Role 관계)을 검사한다. 승인된 요청에 대해 HIS의 LAC로 사용자의 요청정보를 전달한다. ACC와 LAC 간은 상호 신뢰관계(중앙접근제어 에이전트를 통한 사용자의 적합한 요청을 병원정보시스템은 승인)이다. LAC를 통해 ACC로 반환된 데이터에 대해 해당 오브젝트 타입의 기밀/민감 정보에 따른 선택적 암호화를 통해 클라이언트 애플리케이션에 반환하여 선택적 데이터 보호를 제공한다. 특정 HIS에 접근요청을 하는 사용자의 접근제어 검증을 위해 사용되는, 정책 정보(User, Role, User-Role Assignment)는 해당 HIS의 LAC와 동기화 되어있다.

3. 지역접근제어 에이전트 (LAC; Local Access Control Agent)

LAC는 감사 및 사용자 요청에 대한 높은 수준의 접근제어 유효성을 검사한다. LAC은 사용자의 요청의 User-Role 관계 및 HIS의 접근제어 시스템에 의한 Role-Permission 관계를 검증한다. HIS의 데이터에 대한 인가된 사용자의 적합한 요청은, 사용자가 기존 사용자인지 또는 외부 사용자인지 여부를 우선적으로 판별한다. 판별된 사용자는 이중정책 권한관리에 의해 구분되어 접근제어가 이뤄진다. 해당 HIS의 기존 사용자에 대한 접근제어를 위한 내부(사용자) 정책과 속하지 않는 외부 사용자에 대한 접근제어를 위한 외부(사용자) 정책이 있다. LAC는 ACC와 HIS 간의 데이터 변환(Fig. 3, 4)을 담당한다. ACC의 XML 형식의 데이터와 각 HIS의 상이한 형식의 데이터 간의 대응되는 변환을 통해, 클라이언트는 특정 HIS에 독립된 의미적으로 동등한 XML 형식의 데이터를 얻는다. ACC의 요청의 Role을 그 Role에 대응되는 HIS의 User′(Role-Mapped User)로 매핑 변환(Fig. 3) 후, HIS에 사용자의 요청을 전달한다. HIS에 의해 반환된 HIS aware-format 데이터에 대해 ACC aware-format(XML)으로 의미적으로 동등한 구조적 변환(Fig. 4) 수행 후 ACC로 반환한다. 각 HIS의 관리자는(ACC와 HIS 간의 데이

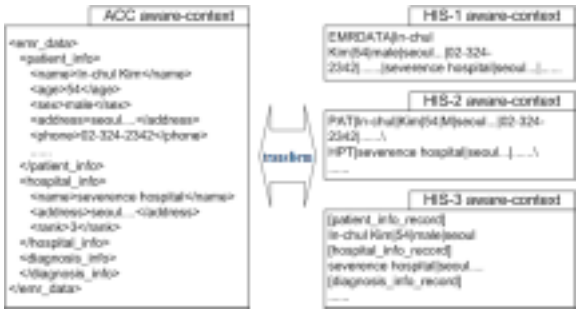

Figure 3. LAC: ACC-HIS data conversion

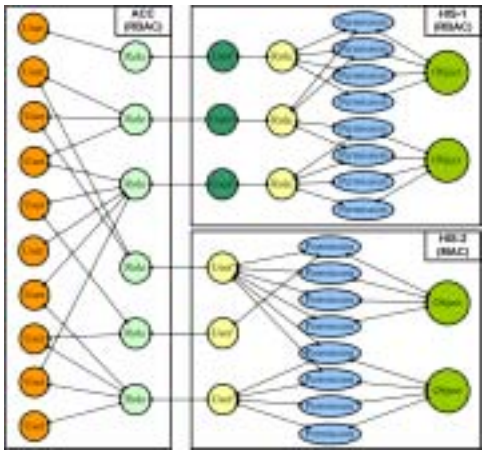

Figure 4. Role of ACC-user' of HIS mapping example

터 변환을 담당하는) 해당 HIS에 속한 LAC를 관리한다.

4. 병원정보시스템 (HIS; Hospital Information System)

HIS는 LAC의 요청에 대한 응답을 한다. 개별적인 전자의무기록 저장소를 갖으며 해당 정책에 따른 사용자 접근제어(R-P 관계 검증)를 한다. 기존 내부 사용자에 대한 접근제어와 외부 사용자에 대한 ACC의 정책의 역할에 대응되는 추가적인 사용자(User'; Role-Mapped User) 리스트를 갖는다.

5. 보안 컴포넌트

사용자 인증(User Authentication)은 사용자의 아이디와 개인 인증서를 통해 검증한다. 접근 제어는 역할기반 접근제어를 통해 사용자의 역할에 따른 병원정보시스템의 전자의무기록에 대한 접근을 제어한다. 데이터 보호를 위해 요청 오브젝트 타입의 민감/기밀 정보에 따른, XML Security를 이용한 선택적 암호화를 통해 중요 데이터에 대한 보호를 제공한다. 네트워크 전송 간 송신자의 개인키를 이용한 전자서명을 첨부하여 전송데이터의 무결성을 보장한다. 또한 로그정보를 유지하여 모든 합법/불법적인 접근, 관리에 대한 감사를 지원한다. ACC의 사용자 인증 프로세스, ACC와 LAC의 접근제어 검증 프로세스/정책 관리 트랜잭션에 대해 로그정보를 남긴다.

IV. 구 현

접근제어 시스템 구축에 있어 XML 기술을 이용하여 역할 기반 접근제어 시스템을 구현하였다. 구현된 시스템에 대한 전체 시스템 구조는(Fig. 1)과 같다.

1. 시스템 구성

대략적인 시스템 요청 프로세스는 클라이언트의

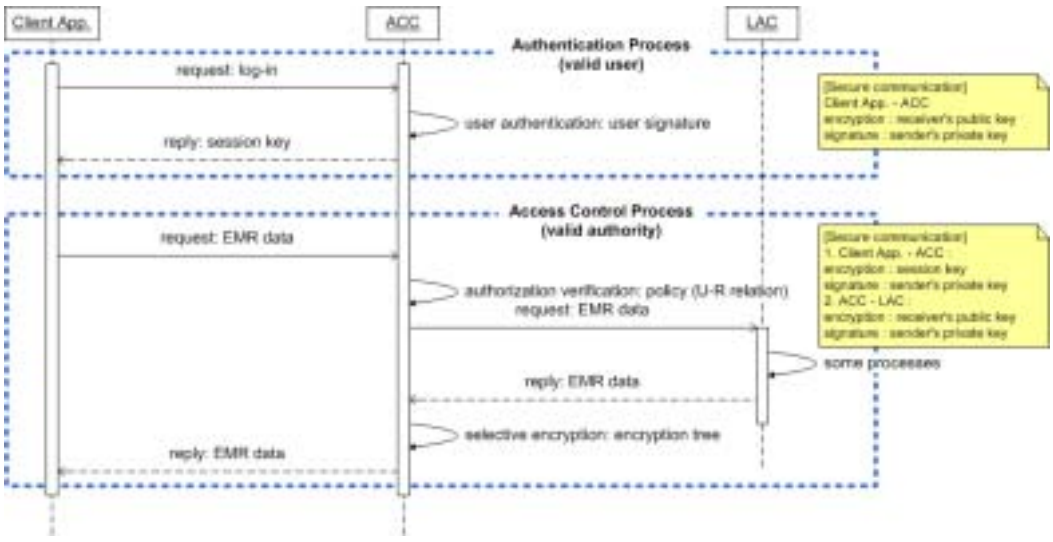

Figure 5. The sequence diagram of process between Client-ACC: Accepted request

사용자 인증 후 중앙접근제어 에이전트(ACC)에 자료를 요청하면, ACC는 사용자 요청의 적합성을 검증 후, 승인된 요청에 대해 그에 따른 적절한 결과 데이터를 반환한다(Fig. 5). 사용자 인증이 실패한 경우와 접근이 거부된 요청에 대해 각각 에러메시지를 클라이언트에게 반환한다. 클라이언트가 ACC에 자료를 요청하는 프로세스는(Table 1)을 따른다. 공개키 기반 X.509v3 인증서를 이용하여 전송 데이터에 대한 전송자의 전자서명을 첨부하여 무결성을 보장하며, 세션키를 이용한 선택적 암호화를 하여 기밀성을 제공한다.

(1) 클라이언트 애플리케이션

사용자는 사용자 아이디와 서명정보를 통해 사용자인증을 하며, 승인된 사용자의 데이터 요청은 다음 튜플로 구성된다.

request := (subject, object, operation)

Table 1. Inquiry process between Client-ACC

① Client: ACC log-in (user authentication)
② Client-ACC: session key setup for secure transmission
③ Client: data request to ACC
④ ACC: suitability verification of request of Client (User-Role relationship)
⑤ ACC: domain (HIS-k) identification of request data
⑥ ACC: (EMR) data request to HIS-k
⑦ ACC: returned data by HIS-k selectively encrypts with session key and replies to Client
⑧ Client : decrypts and confirms data

각 element에 대한 설명은 Table 2와 같다.

요청 정보는 사용자의 전자서명 정보를 첨부하여 ACC로 전송하여 요청문에 대한 무결성을 제공한다. ACC에 대한 요청 응답은 다음과 같다.

respond := (valid_response | invalid_response)
valid_response:= (request, selective_encrypted_data)
invalid_response := (request, error_message)
selective_encrypted_data : 선택적 암호화된 EMR data
error_message : 거부된 요청에 대한 에러 메시지

위 응답에 ACC의 전자서명을 덧붙여 데이터에 무결성을 제공한다.

(2) 중앙접근제어 에이전트(ACC)

ACC는 클라이언트의 사용자 인증 후, 전송된 요청의 적합성을 검증(Fig. 6. URVerification)한다. 사용자-역할(U-R) 관계 검증이 승인되면 (요청 데이터가 있는 HIS의) LAC로 요청을 전달(request-Data)한다. LAC는 응답 결과를 ACC로 반환한다. 반환된 데이터와 데이터의 오브젝트 타입에 따른 암호화 트리(getEncryptionTree)의 민감/기밀성 정보에 따라 선택적 암호화된 최종 결과 데이터를 생성한다(getFinalData, Fig. 7). 선택적 암호화된 결과 데이터에 ACC의 전자서명을 첨부하여 클라이언트로 전송한다. ACC의 저장소(Repository)는 클라이

Table 2. Tuple syntax of Client's request(using EBNF Syntax)

Element	Sub-element
Subject	(User Id, Domain, Role)
User Id	User identifier
Domain	HIS identifier
Role	User role (ex) doctor, nurse, patient etc.)
Object	(Object type, Object Id, Range)
Object type	Type of user request data (ex) diagnosis, PACS..)
Object Id	Identifier of user request data
Range	Locator following XML XPath expression15)
Operation	(Read | Write | Create | Delete)

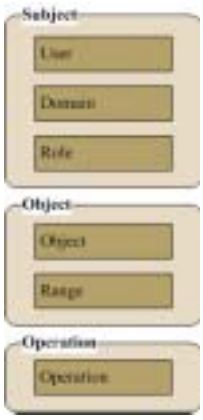

Figure 7. The state diagram of ACC agent

언트와 LAC의 공개키 정보를 갖는 키 데이터베이스와 접근 정책 정보를 갖는 정책 데이터베이스, 사용자의 접근 로그정보를 저장하는 로그 데이터베이스로 구성된다. 정책 데이터베이스는 User, Role, U-R Assignment 정보와 요청 데이터의 객체 타입별 암호화되어야 하는 노드에 대한 정보를 갖는다.

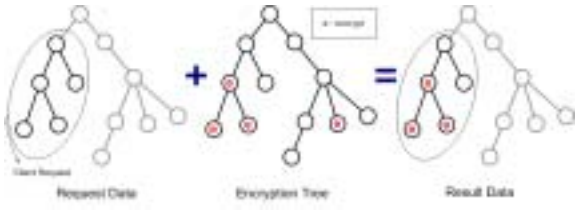

Figure 8. Request data, encryption tree, result data

(3) 지역접근제어 에이전트 (LAC)

전체 LAC과 HIS 간의 프로세스는 Figure 8을 따른다.

LAC은 ACC에서 전달된 요청(Fig. 9. receive Request)의 적합성을 재검증(verifyRequest)한다. 사용자-역할(U-R) 관계 검증이 승인되면, ACC의 Role에 해당하는 HIS의 User′(Role-Mapped User)와의 매핑 변환(Fig. 3)한다. 또한 사용자의 요청을 각 HIS에 종속된 요청 형식으로 변환(transform Request)한다. 변환된 요청을 HIS로 전달(getData)한다. HIS에 의해 반환된 요청에 대해 ACC가 이해하는 포맷으로 변환을 수행(transformData, Fig. 4)한다. 변환된 데이터는 ACC에게 반환된다(sendData). LAC은 ACC에게는 HIS이며, HIS에게는 기존 HIS를 이용하는 클라이언트와 같다. LAC은 클라이언트의 HIS에 대한 접근제어를 위해 User, Role, U-R Assignment 정보를 갖는 Policy Database를 갖는다. 매핑변환을 위해 R-U′ Assignment Database 및 관

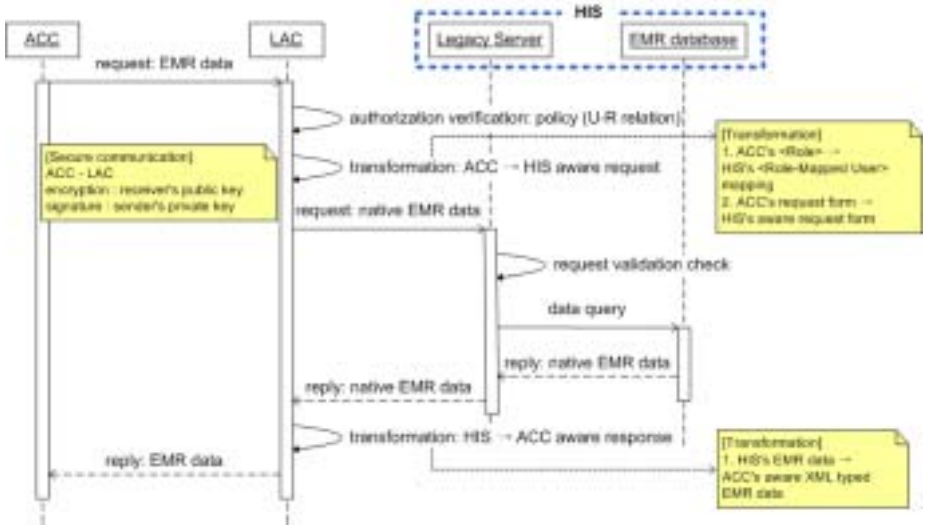

Figure 9. The sequence diagram of process between LAC-HIS

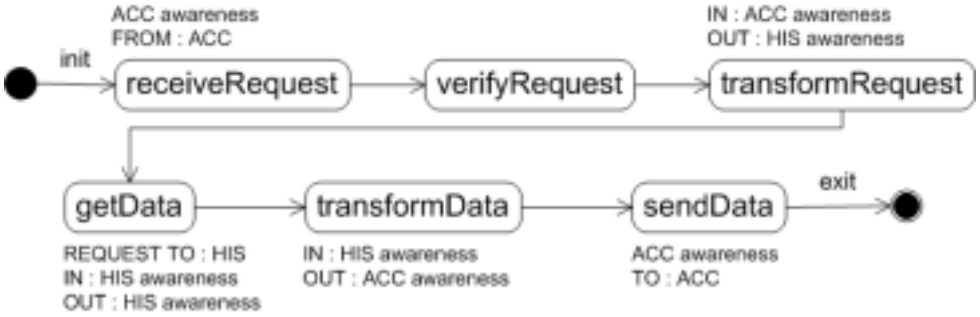

Figure 10. The state diagram of LAC agent

련된 매핑 테이블을 갖는다.

⑷ 병원정보시스템(HIS):
섹션 Ⅲ.4와 동일

2. 보안 서비스 구성

⑴ 암호화 서비스

월드와이드웹 컨소시엄(W3C) 권고안인 XML 기술을 이용한 XML-Signature와 XML Encryption는 XML로 기술된 데이터의 선택적인 암호화와 전자서명에 유용하다. 본 논문에서는 암/복호화 및 전자서명을 위한 키로(공개키 방식의 공인인증서 규격인) X.509v3 인증서를 이용하였다. 전자서명 해쉬 알고리즘으로는 SHA-1을 사용하였고 암호화 알고리즘으로 비대칭키 알고리즘인 RSA, 대칭키 알고리즘인 3-DES를 이용하였다. RSA를 이용한 암호화는 강력한 보안을 제공하지만 매우 커다란 숫자들에 대한 지수 연산을 수행하기 때문에 시스템 부하가 높은 단점이 있다. 따라서 비교적 강력한 3-DES 암호화 알고리즘을 사용하는 세션키를 이용하여 데이터를 암호화한다. 데이터 암호화에 사용된 세션키는 RSA 알고리즘으로 암호화하여 키를 보호한다. 기밀 데이터에 대한 암/복호화로 인한 전체 시스템 처리 시간을 줄였다.

⑵ 접근제어 서비스

ACC의 접근제어는 Figure 5의 URVerification을 통해 사용자-역할 관계를 검증하여 접근제어 한다. 접근제어를 위한 정책은 다음 튜플로 구성된다.

policy := (access_policy, encryption_policy)
access_policy := (user*, role*, user_role_assignment*)
encryption_policy := (object_type, encryption_tree_info)*
user_role_assignment := (ref_user, ref_role)
user : 사용자 식별자
role : 역할 식별자
ref_user : user 참조 식별자
ref_role : role 참조 식별자
object_type : 객체 타입 (예) 진단서, 청구서, PACS 이미지 등)
encryption_tree_info : 객체 타입의 암호화 여부에 대한 상세정보를 갖는 자료구조

ACC의 접근제어 정책은 접근제어를 위한 access_policy와 데이터의 민감/기밀 정보를 갖는 encryption_policy로 구성된다. access_policy는 역할기반 접근제어(RBAC) 시스템을 구성하는 user, role 정보와 U-R 관계 정보를 정의한다. encryption_policy는 사용자가 요청하는 object type에 따른 민감/기밀 정보를 정의한다. LAC의 접근제어는 (Fig. 8)의 verifyRequest 단계에서 제어가 이루어지며 접근제어를 위한 정책은 다음 튜플로 구성된다.

policy := (access_policy, role_mapping)
role_mapping := (role, role_mapped_user)
role_mapped_user : ACC의 역할에 대응되는 HIS의 Role-Mapped User

LAC의 접근제어 정책은 접근제어를 위한 access_

policy와 데이터 요청의 변환 매핑정보를 갖는 role_mapping으로 구성된다.

V. 결 과

사용자 인증 및 허가된 역할 기반 접근제어를 통한 Multi-HIS에 접근하는 사용자의 요청은 ACC가 중앙에서 제어한다. 기존 HIS을 이용하는 사용자에게는 동일 접근권한을 갖는 내부정책으로 해당 HIS를 이용할 수 있으며, 외부의 사용자에 대해서는 외부정책을 통해 구분된 이중 권한관리를 한다. 사용자의 요청 데이터는 데이터를 받아오는 해당 HIS와 상관없이 XML로 기술된 동일한 형식을 사용자에게 제공하며, XSLT를 이용한 사용자 친화적인 뷰를 제공한다. 클라이언트에게는 ACC가 HIS로 보인다. 클라이언트 애플리케이션은 여러 HIS에 대한 동일한 사용자 인터페이스를 제공한다. 상기 시스템에 대한 다음과 같은 시나리오를 적용해 볼 수 있다.

시나리오 1. 병원 A에서 병원 B의 환자 O의 진료기록 검색

환자 O를 담당하는 병원 A의 의사 C는 환자가 이전에 다니던 병원 B의 진료기록을 토대로 환자에 대한 적절한 진료를 하기 위해 접근제어 에이전트를 통해 환자 O의 담당의사의 역할을 이용하여, 병원 B의 환자 O의 진료기록을 살펴볼 수 있었다. 이를 통해 환자의 최근 증상에 대한 복합적인 적절한 처방을 내릴 수 있었다.

시나리오 2. 원무환자 O의 병원 A에서의 진료 결과 조회

원무환자 O는 최근 자신의 몸이 이상증상을 느껴 병원 A에 들러 진단을 받았지만, 곧 업무로 인한 해외 출장을 가게 되었다. 출장기간 동안 자신의 증상에 대한 걱정에 접근제어 에이전트를 통해 자신의 진단기록을 살펴보고 단지 피로가 쌓여 생긴 것임을 알 수 있어 안정을 되찾을 수 있었다. 처방과 관련하여 고혈압 증상이 있으므로 최근 동안은 술을 피하라는 권고를 받아들였다.

시나리오 3. 병원 간 협력적 진료

병원 A의 의사 O는 자신이 맡은 환자 P의 증상이 희귀하여, 우선 접근제어 에이전트를 통한 리서처의 역할을 이용하여 해당 증상에 대한 타 병원들의 자료를 수집하여 환자 P의 증상과 비슷한 경우에 대한 관련 사례들을 얻을 수 있었다.

VI. 고 찰

제안된 시스템은 클라이언트 애플리케이션과 여러 HIS를 접근제어 하는 ACC, 각 HIS와 ACC 간의 통신을 가능케 하는 LAC, HIS의 4-티어 구조로 되어있다. 기존에 제안된 병원정보시스템의 정보교환을 위한 1:m의 신뢰관계[3)4)]는 ACC를 통한 1:1의 관계가 된다. 각 병원정보시스템은 ACC에 등록 추가/삭제되며, 각 병원정보시스템간의 정보공유는 ACC를 통해서 이뤄진다. 이를 통해 각 병원정보시스템의 정보공유는 유연성을 얻는다. 사용자는 ACC와 통신하며 ACC를 통해 각 병원정보시스템의 의료데이터를 얻는다. 적합한 권한을 갖는 사용자는 장소에 상관없이 동일한 접근 인터페이스를 통해 여러 상이한 플랫폼으로 구성된 HIS의 의료데이터에 접근 가능하다. 각 HIS의 상이한 접근제어시스템은 LAC의 변환과정을 통해 ACC의 RBAC 시스템으로 통합되어 접근 제어된다. 또한 공통 데이터 포맷을 사용하여 데이터는 각 HIS 시스템에 독립된다. 사용자가 접근 요청하는 ACC와 LAC는 웹서비스로 구현이 되었다. 웹서비스는 XML 기반의 SOAP 메시지를 사용하며, HTTP 프로토콜을 사용하여 기존의 방화벽을 건드리지 않는다[10)16)]. 그리고 서비스 지향 컴포넌트 기술로 재사용성이 높다. 웹서비스는 웹기반의 플랫폼 독립적인 기술로, 기존 HIS의 플랫폼에 상관없이 구현, 사용할 수 있다. LAC의 모듈화는 ACC에 신규 HIS의 추가, 삭제를 용이하게 하여 확장성 및 유연성을 보장한다. 일부 기밀성이 요구되는 EMR 데이터에 대해 XML 암호화 기술을 이용하여 암호화 효율을 높인다. 통합된 접근제어 관리와 전송 간의 공통 데이터 포맷을 사용하여 각 병원간 협력적 진료를 돕는다. 이를 통해 사용자는 플랫폼 독립성과 장소에 독립되어 자유로운 접근성을 보장받는다. 제안된 시스템은 조회를 기본으로 설계되었고 다양한 작업에 대한 트랜잭션을 지원하도록 개선되어야 한다. ACC에서 사용되는 공통 데이터 형

식은 표준화를 위해 제안되는 HL7을 지원하도록 개선함으로써 기존 시스템이 표준시스템으로 이전하는 것을 용이하게 할 수 있다.

참고문헌

1. Weiss G. Welcome To The (Almost) Digital Hospital. Spectrum, IEEE 2002;39(3):44-49.
2. Coile RC. The Paperless Hospital: Healthcare in a Digital Age. Health Admin Press;2002.
3. Gritzalis D, Lambrinoudakis C. A security architecture for interconnecting health information systems. Int J Med Inf 2004;73(3):305-309.
4. Kallepalli VN, Ehikioya SA, Camorlinga S, Rueda JA. Security middleware infrastructure for DICOM images in health information systems. J Digit Imaging 2003;16(4):356-364.
5. Scott RE, Jennett P, Yeo M. Access and authorisation in a Glocal e-Health Policy context. Int J Med Inf 2004;73(3):259-266.
6. Blobel B. Authorisation and access control for electronic health record systems. Int J Med Inf 2004;73(3):251-257.
7. Tzelepi S, Pangalos G, Nikolacopoulou G. Security of medical multimedia. Med Inform Internet Med 2002;27(3):169-184.
8. Bhatti R, Joshi JBD, Bertino E, Ghafoor A. Access control in dynamic XML-based web-service with X-RBAC. ACM 2003.
9. Ferraiolo DF, Kuhn DR, Chandramouli R. Role-Based Access Control. 1st ed. Artech House 2003:16-18.
10. Takase T, Uramoto N, Baba K. XML digital signature system independent of existing applications. Symposium on Applications and the Internet(SAINT) 2002:150-157.
11. Dournaee B. XML security. 1st ed. McGraw-Hill 2002:107-278.
12. Available at: http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/. Accessed July 10, 2004
13. Available at: http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/. Accessed July 10, 2004
14. Available at: http://www.ietf.org/rfc/rfc3280.txt. Accessed July 10, 2004
15. Available at: http://www.w3.org/TR/1999/REC-xpath-19991116/. Accessed July 10, 2004
16. Available at: http://www.w3.org/TR/soap12/. Accessed July 10, 2004