모바일 환경의 원격의료 인증 시스템

오근탁° 김경주 이윤배 이성태 이영신
조선대학교 전자계산학과
{gtoh°, kgkim, yblee, stlee, yslee}@chosun.ac.kr

Remote Medical Authentication System on the Mobile Environment

GuanTack Oh° Kungju Kim YunBae Lee SungTae Lee YungSin Lee
Dept. of Computer Engineering, Chosun University, Gwangju, Korea

요 약

오늘날 원격 환경의 진료시스템이 개발되고 있는데, 이들 시스템은 미래의 원격진료 즉, 병원에 직접가지 않고 집에서 바로 혈압, 심박수 등을 검사 받을 수 있는 시스템 개발의 기본이 되고 있다. 그리고 정보통신의 발전으로 모바일 PC 즉, 개인 휴대용 단말기(PDA:Personal Digital Assistants)가 의료분야에서 PC를 대체하여 이동성, 편리성을 제공하는 전자 차트를 선보이고 있다. 그러나 PDA는 작은 몸체로 이동성 및 편리성 등이 PC보다 뛰어나지만, 해상도가 큰 이미지, 높은 처리 속도를 요구하는 작업 등을 처리하기에는 효율성이 낮은 문제점이 있다. 또한 정보를 공유 할 수 있는 데이터를 무선 환경으로 처리해야 하기 때문에 환자와 관련된 의료 영상 즉, MRI 사진이나 X-ray 사진 등을 의료 환경에 이용 하는 데는 보안 의 문제점을 가지고 있다 따라서 본 논문에서는 매우 빠르게 발전하고 있는 진단과 치료기술을 이러한 의료를 필요로 하는 사람들에게 제공하는 접근성의 보장 문제를 해결할 수 있는 대안으로 원격의료 인증시스템을 제안 하고자 한다.

1. 서 론

현재 네트워크 기술 발전으로 인하여 거의 모든 곳에 네트워크가 보급 되면서 학교, 병원 등의 건물 내에서도 네트워크에 연결하여 인터넷 접속 및 네트워크 작업 등을 할 수 있게 됐다. 또한, 인터넷을 통한 멀티미디어 기술이 발달되어 의료분야, 전자.전기 분야 등에 걸쳐 많은 기여를 하였다. 그래서 병원에서도 실시간으로 치료 및 진찰을 할 수 있는 원격진료시스템이 개발 되어 의사나 담당 간호사의 PC를 이용하여 환자의 정보, X-ray 촬영 사진 등을 담은 차트를 검색하고, 볼 수 있는 환경이 가능하게 되었다. 이런 원격의료시스템에 대한 연구는 현재 많은 곳에서 이루어지고 있지만, 실제 임상에서 사용되기 위해서는 이동성과 무선 환경의 데이터 교환으로 인한 보안의 문제가 발생하고 있다.

예를 들어, 지금 바로 수술에 들어가야 하는 환자가 있는데, 그 환자에 대한 기록과 CT촬영 같은 자료를 보기 위해서 다시 자신의 PC로 돌아가야 한다는 것이다. 물론 이동성을 위한 노트북과 같은 컴퓨터가 있지만, 아직 이동하기에는 무겁고, 일정한 공간을 차지하기는 마찬가지 이다.
그러므로 이 논문은 무선 네트워크기반으로 모바일 컴퓨터용 아키텍쳐인 WAP를 이용하여 휴대용 정보단말기인 PDA를 통해 임상에 필요한 데이터를 전송받아 실시간으로 환자에게 처방을 할 수 있는 시스템을 연구하였고 자료를 전송받는 도중에 발생할 수 있는 보안 문제를 인증시스템을 도입하여 의료분야에 기여할 수 있도록 제안한다.

2. 관련연구

2.1 WAP기반의 모바일 통신

WAP(Wireless Application Protocol)는 모든 무선 네트워크에 연결할 수 있는 모바일 컴퓨터용 아키텍처로 현재 많은 기업체에서 이것을 기반으로 모바일 환경에서 브라우저를 이용하여 데이터 전송 및 인터넷 서비스를 제공하고 있다.

2.2 WAP에서 Server와 PDA간의 구조

WAP Gateway를 통하여 그림 1처럼 Server에서 HTTP나 FTP등이 TCP/IP를 통하여 WAP Gateway에 전송되며, WAP Gateway는 WSP, WTP등으로 변환하여 각 단말기인 Client에게 WDP를 이용하여 전송하게 되어 PDA의 브라우져로 볼 수 있다. 또, 환자에게 처방 같이 Server에 데이터를 전송해야하는 경우에도 위와 같은 구조로 전송하게 된다.

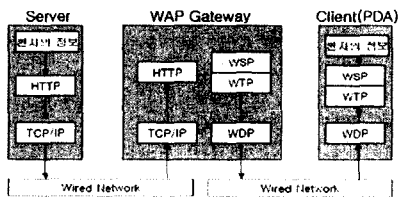

그림 1. SEVER와 PDA간의 구조

모바일에서의 원격진료시스템 구성

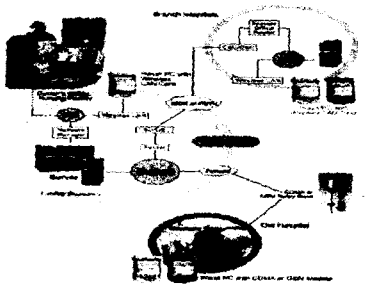

그림 2 모바일에서의 원격진료시스템 구성

3. 원격 진료 시스템

3.1 시스템 구성

WAP을 기반으로 한 원격 진료시스템을 구현을 위해서 먼저 전체의 구조를 파악이 중요하다. 새로운 환자를 입력하면 DB Ser
ver에 저장이 되고, Webserver를 통하여 각각 필요한 의사, 간호사의 PC에 전송이 된다. 그리고 처방전이나 X-ray 촬영 등의 새로운 데이터를 입력하면 바로 Server 전송되어 저장된다.
이 기본 구조에 그림 2와 같이 PDA Client를 접합시켜 PDA에서도 검색, Update등을 할 수 있는 구조를 가져야 한다.

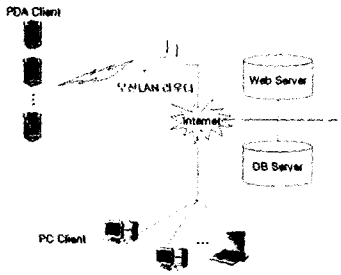

그림 3. PDA Client를 추가한 원격진료 시스템의 네트워크 구조

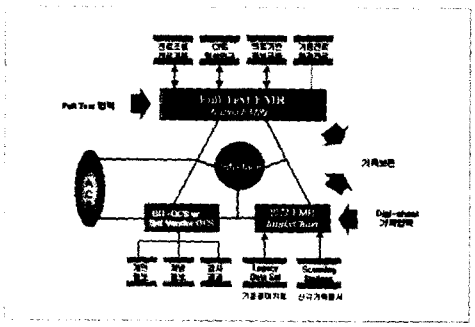

그림4. PAD를 이용한 병원의료정보 구성도

3.2 WAP의 구조

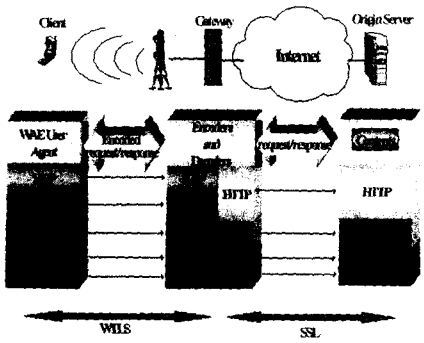

그림 5. WAP의 구조

3.3 WAP의 보안

무선구간 (WTLS (TLS) : 사용자로부터 전달된 데이터를 해독하고 다시 암호화 하여 웹 서버로 전달유선구간 (TLS (WTLS) : 웹 서버로 부터 전달된 데이터를 해독하고 이를 다시 암호화 하여 사용자에게 전달한다. 이 과정에서 WAP G/W는 사용자와 서버간 전달되는 데이터의 모든 내용을 해독. 보안의 허점이 노출되어 유선인터넷과 같은 완벽한 END-TO-END 보안을 제공 하지 못한다. 따라서 본 논문에서는 두 가지 방법에서 살펴보았다.

4. 제안 시스템

대안1: 응용수준에서 암호화를 수행하는 방법

서버의 인증서를 가져와 세션키를 암호화 하여 암호문과 함께 전송하는 방식으로 WAP 규격에서 지원하지 않는 사설방식이다.

대안 2: Secure Domain

응용 서버가 신뢰하는 GATEWAY를 직접 운영하는 Secure Domain을 사용하면WAP 표준의 WTLS를 이용하여 신뢰할 수 있는 Client authentication 및 기밀성 보장이 가능하다.

이 해결 방안으로 WPKI 를 제시한다.

WPKI 구조는 다음과 같다

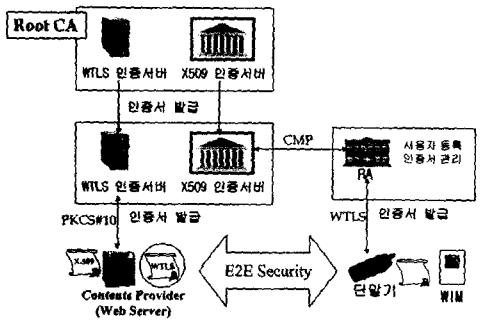

그림 6 WPKI 구조도

WPKI 인증서의 종류는 다음과 같다

WAP G/W 인증서

WTLS 서버인증용(minicert) 무선 사업자가 운영하는 WAP Gateway에 발급 무선으로 단말기에 전송한다.
사용자 및 서비수서버 인증서 WTLS 클라이언트 인증용(X.509 cert) 단말기에는 URL만 저장하고 WTLS 서버가 인 증시 디렉터리에서 가져온다.
전자서명용 (x.509 cert) 단말기에는 URL 만 저장하고 응용 서버가 서명 검증시 해당 디렉터리에서 가져온다.

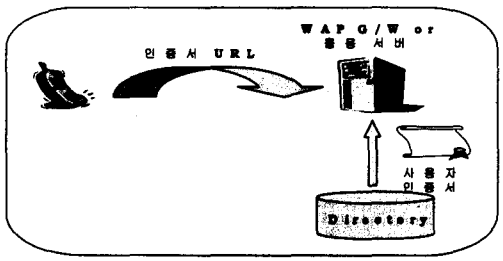

그림 7 WPKI 인증서 구조 절차도

WPKI 구현 문제점 및 해결방안

CA 인증서 무결성 확인이 어려우므로 단말기에 데이터를 전송할 때CA 인증서를 전송 설치한다.

X.509 CRL 방식의 CRL목록을 이용한 인증서 검증이 어려우므로 서버는 Short-lived 인증서를 사용하였다

유무선 연동을 고려하여 다음과 같은 사항을 추가 하였다.

유선 : RSA기반의 X.509 v3 인증서

무선 : ECC 기반의 WTLS 및 X.509

인증서

단말기에서는 RSA와 ECC를 동시 지원하고 서버는 WTLS 및 X.509 인증서를 복수 발행하여 해결하였다.

키 생성 암호화
낮은 단말기 성능에 따른 기존 RSA 1024bit 사용이 어렵다 따라서 ECC 알고리즘을 사용하였다..

5. 구현

WAP기반에서의 PDA를 이용한 원격 진료 시스템의 모듈을 구현하는 개발 환경은 다음과 같다.

사용기종: 펜티엄 III IG
운영체제: WINDOWS 2000 SERVER
개발도구: VISUAL C++ 6.0, JAVA

개발환경의 프로그램 모듈은 다음과 같다

```
package Stock;
import javax.microedition.lcdui.*;import java.io.*;
public class MenuCanvas extends Canvas{
private Image off_bg, on_bg;private int
selected_menu;private Display display;private
InterestCanvas interest_cvs;
public MenuCanvas(Display display) throws
IOException{
g.drawImage(on_bg,
getWidth()/2,20Graphics.HCENTER|Graphics.TOP);g.dr
awImage(off_bg, getWidth()/2, 40,
Graphics.HCENTER|Graphics.TOP);g.drawImage(off_b
g, getWidth()/2, ,Graphics.HCENTER|Graphics.TOP);
g.drawImage(off_bg, getWidth()/2,80,
Graphics.HCENTER|Graphics.TOP);
g.drawImage(off_bg, getWidth()/2, 90,
Graphics.HCENTER|Graphics.TOP);
 }
}
```

6. 결론 및 향후 연구 과제

오늘날 원격의료가 새롭게 부각되는 것은 보통신기술의 발달이 원격의료를 뒷받침해 주고 있기 때문이기도 면서 새로운 의료서비스에 대한 제공자와 수요자들의 전환이 이루어지고 있기 때문이라고 할 수 있다. 매우 빠르게 발전하고 있는 진단과 치료기술을 이러한 의료를 필요로 하는 사람들에게 제공하는 접근성의 보장 문제를 해결할 수 있는 대안으로 원격의료가 떠오르고 있다. 원격의료의 도입 배경 역시 통신과 네트워킹 기술의 고도화를 기반으로 하여 원격영상기술, 원격자료전송 기술 등의 신기술이 개발되면서 본격화되기 시작하였다
원격의료가 환자, 의사 및 의료기관, 그리고 사회전체에 미치게 될 여러 가지 긍정적 효과들이 예상되면서 이에 대한 활발한 연구와 보안 관련 사업들의 추진이 전 세계적 으로 펼쳐지고 있다. 원격의료의 도입을 활성화의 원동력이 되고 있는 원격의료 인증 시스템 도입의 긍정적 효과는 사회적으로 미치는 효과는 대단하다 할수 있다.
먼저 환자에게 미치는 영향을 살펴보면, 원격의료가 확대되면 벽지에 거주하는 지역주민은 원격에 있는 대학병원 전문의로부터 의료서비스를 받을 수 있게 된다. 위치에 관계없이 다른 병원이나, 의료진과 상담을 하더라도 진료를 위한 검사의 불필요한 중복도 피할 수 있다. 환자는 의사와 각종 의료 기기가 있는 병원 등에 가지 않더라도, 단지 의사가 치료를 위한 결정을 내릴 수 있도록 적절한 시간 내에 필요한 정보가 전송되면 된다. 거동이 불편한 환자를 위한 재택진료를 통해 환자의 가정에서 전문의가 직접 그리고 저렴한 비용으로 진료를 할 수 있다. 즉 가장 적절한 수준의 진료가 가능할 것이다. 또한 원격자문을 하게 되면 현지 의사에게 원격지 의사로부터 추가의견을 들을 수 있으므로 오진의 위험도 줄어드는 등 의료서비스의 질 향상 효과도 있을 수 있다. 따라서 원격 진료 시스템을 이용하면 거리, 시간, 재정적인 제한을 감소하여 환자들의 의료기관에 대한 신뢰감을 향상시킬 수 있다.

6. 참고문헌

[1]Marchin Metter, "WAP enabling existing HTML applications", IEEE AUIC, Jan 31, 2000.

[2]Rick Bender, "Kentucky Field Inspection PDA Application" , IPEC, Conf2002, 2002.

[3] Jo & S 기획 저, "모바일 프로그래밍", 2002.

[4] 홍준호 외 2인 공저, "about WAP" 2001.