JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 1 : 205~214 Jan. 2017

스마트 헬스케어 서비스를 위한 홍채인식기반의 원격의료시스템

조영복[1] · 우성희[2*] · 이상호[1] · 김민경[3]

A Secure Telemedicine System for Smart Healthcare Service

Young-bok Cho[1] · Sung-Hee Woo[2*] · Sang-Ho Lee[1] · Min-Kang Kim[3]

[1]Department of Computer Science, Chungbuk National University, Chungbuk 28644, Korea
[2*]Department of Medical Information&Engineering, Korea National University of Transportation, Chungbuk, 27469, Korea
[3]Department of Research & Development Center, SONOUM Inc., Chungbuk, 28501, Korea

요 약

이 논문에서는 스마트 헬스케어 서비스를 위한 홍채인증기반 안전한 원격의료 시스템을 제안한다. 원격의료 시스템에서는 의료정보 및 헬스케어 정보는 프라이버시 정보로 매우 중요한 정보이다. 이 논문에서 제안 시스템은 노인성 만성질환 환자들을 위한 원격의료 시스템으로 기존 ID/PW방식보다 편리하면서 안전한 인증방식을 제공한다. 노인성만성질환자의 사용 편의성과 의료 환경의 특수성을 고려했을 경우 제안방식은 적합한 인증수단으로 타인에게 도용되거나 분실시 쉽게 변경하기 어려워 기존 ID/PW방식에 비해 안전하다. 또한 스마트헬스케어서비스를 위한 원격의료 시스템은 의료정보 및 헬스케어 정보의 민감한 프라이버시 유형중 하나로 원격의료 시스템에서 매우 중요한 보안요구사항 중 하나이다. 따라서 우리는 제안 논문에서 민감한 의료정보 및 개인정보 보호를 제공하는 2단계 인증 프로토콜을 제시하였다. 제안 방식은 기존 ID/PW방식보다 높은 기밀성과 무결성을 제공하며 보다 강력한 안전성을 제공함을 증명하였다.

ABSTRACT

In this paper, we proposed an iris-based authentication for smart healthcare service in secure telemedicine system. The medical and healthcare information's are very important data in telemedicine system from privacy information. thus, the proposed system provides a secure and convenient authentication method than the traditional ID/PW authentication method to a telemedicine system for age-related chronic diseases. When considering the peculiarities of the use of age-related chronic diseases convenience and healthcare environments, the proposed approach is difficult to secure than traditional ID/PW authentication method with the appropriate means to easily change when stolen or lost to others. In addition, the telemedicine system for the smart healthcare services is one of the types of privacy sensitive medical and health data. it is very important security needs in telemedicine system. Thus we protocol are offer high confidentiality and integrity than existing ID/PW method.

키워드 : 스마트 헬스케어, 원격의료 시스템, 모바일 의료정보 , 홍채인증

Key word : Smart Healthcare, Remote Medical System, Mobile Medical Information, Iris Authentication

Received 11 October 2016, **Revised** 03 November 2016, **Accepted** 06 December 2016

* **Corresponding Author** Sung-Hee Woo(E-mail:shwoo@ut.ac.kr, Tel:+82-43-820-5323)
Department of Medical Information&Engineering, Korea National University of Transportation, Chungbuk 27469, Korea

Open Access http://doi.org/10.6109/jkiice.2017.21.1.205 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

IT의 발달과 더불어 컴퓨팅 사업을 융합하는 연재의 추세에 따라 컴퓨팅의 개념을 도입하여 원격의료기술을 활용한 건강관리 서비스 즉 스마트 헬스케어를 위한 안전한 원격의료 시스템을 활용한 개인 건강관리 서비스모델이 제시되어야 할 필요성이 있다. 현재까지는 유비쿼터스 컴퓨팅을 기반으로 원격 헬스케어 서비스 모델이 제시되고 있고 원격 헬스케어 서비스 모델은 의료정보화를 통한 의료서비스 질의 향상, 생산성과 작업의 효율화, 의료사고의 감소 등을 목표로 하고 있다[1,2]. 스마트 헬스케어 서비스 산업이 활성화되기 위해서 개인의 진료정보 보관 및 관리가 중요하다. 현재 의료기관에서 진료기록을 관리하는 방법에 문제점이 많고 의료기관별로 정보가 분산되어 있어 환자가 아닌 의료기관 중심으로 관리되고 있으며 환자가 필요시 접근이 불가능하다는 문제점을 가지고 있다. 또한 표준화 작업이 필요한 시점으로 의료기관 중심이 아닌 환자 중심의 표준화 작업이 시급하다. 따라서 언제, 어디서나 대인 진료기록에 접근할 수 있고 중복 검사를 방지하며 환자의 평생 건강 기록(PHR : Personal Health Record)을 보호하고 개인의 진료 정보를 의료기관이 공동으로 활용할 수 있도록 개선이 필요하다[3,4]. 또한 스마트 헬스케어 서비스를 위해 컴퓨팅 서비스의 보안 요구사항들이 만족 할 수 있도록 개인 의료 정보보안 요구조건이 공유되어야 하며 정확한 진료를 위해서 정보의 공유 및 2차 활용이 필수적이다. 이러한 정보의 공유로 인한 보안상 취약성이 및 정보노출로 인한 스마트 헬스케어 원격의료 시스템에 대한 보안상 문제점이 제기되고 있고[3,5] 이는 심각한 제3자에게 환자의 정보가 노출되고 있는 문제점이 지적되고 있다. 따라서 개인의료 데이터에 대한 접근 권한을 제어할 수 있는 기능이 필요할 경우 환자의 동의에 따라 개인의료정보 PHR의 안전한 공유 및 활용을 요구하고 암호화를 통한 스마트 기반의 헬스케어 서비스를 위한 안전한 원격의료 시스템 모델이 필요하다. 이 논문에서는 스마트 헬스케어 서비스를 위한 안전한 원격의료 시스템을 제공하기 위한 시스템 모델을 제안하고 제안 모델에서는 환자의 프라이버시 보호와 환자의 의료기록 즉 PHR 접근을 위한 상황(context), 부정적인 허가(negative permission), 의무(obligation)의 개념을 포함한다.

이 논문의 구성은 2장에서는 관련연구로 스마트 헬스케어의 동향에 대해 기술하고 3장에서는 제안하는 스마트 헬스케어 서비스를 위한 안전한 원격의료 시스템 모델을 제안하고 한다. 4장에서는 제안 하는 모델의 안전성을 평가하고 5장에서는 결론과 향후 발전방향을 기술한다.

Ⅱ. 본 론

2.1. 스마트 헬스케어 서비스의 필요성

전 세계적으로 만성질환(Chronic Disease)이 급격하게 증가하고 있으며, 고령화 사회의 진입과 건강에 대한 관심이 높아지고 있다[1]. 이에 따라 의료서비스의 전문화와 다양화를 통한 개인 맞춤형 의료 서비스가 요구되고 있으며, 기존의 병원 방문을 통한 의료체제에서 질병 예방의 사후 관리와 맞춤형 서비스와 같은 새로운 의료서비스의 수요가 증대하고 있다[6]. 이와 더불어 고령 인구화와 생활수준 향상으로 생활패턴의 변화가 과거에 비해 당뇨, 고혈압, 고지혈증 등 만성질환이 급속도로 증가하고 있으며 이에 따른 의료비용이 향후 사회적인 부담으로 크게 작용하고 있다. 우리나라의 총 의료비 지출은 (2003년 40조원 수준) GDP 대비 5.6%로 여타 OECD 국가에 비해 낮은 수준이지만 선진국의 경우 이미 만성질환 관련 의료비용이 전체 의료비의 50%를 초과하고 있는 실정이다. 다음 표 1은 주요 국가별 총 의료비 지출 규모를 나타낸 것이다.

Table. 1 Major national total medical expenditure

	USA	UK	FR	DE	JP	KR
Total	1,720	126	186	277	328	40
GDP rate(%)	15.0	7.7	10.1	11.1	7.9	5.6

스마트 헬스케어는 언제 · 어디서나 환자의 상태를 지능적으로 모니터링하면서 관리하고 환자 정보와 질병 정보등을 분석하여 실시간으로 맞춤형 서비스가 제공되는 것으로 의료서비스와 건강관리 서비스가 모두 제공되어 의료비스를 요구하는 환자는 물론 건강에 관심을 가지고 있는 일반인 대상의 상시적인 케어(care) 서비스와 필요에 따라 제공되는 의료서비스를 포함하

고 있는 것이다. 즉 스마트 헬스케어는 스마트, 빅 데이터, 소셜 네트워크를 모두 포함하는 개념으로 스마트 헬스의 특징을 한국정보화진흥원에서는 스마트 공공보건의료 서비스 도입방안으로 지능적으로 분석된 정보의 전달이 지식에서 지혜로 변화는 과정에 있는 형태로 지능형 · 맞춤형 헬스케어서비스가 이루어지는, 즉 지식과 지혜가 혼재된 정보전달 형태, 모든 헬스케어 서비스에 완전한 , 완성된, 안전한, 표준화된 보안된 스마트 IT 기술 적용, 스마트시대의 헬스케어서비스는 의료와 복지, 안전등이 복합되어 제공, 수요자와 공급자의 구분이 없어져가는 상태, 즉 프로슈머의 진행상태, 상호전달 된 정보나 지식(PHR)은 사례 기반추론(CBR)을 통해 재사용되고 새로운 지식으로 생산되어 지식이 끈임 없이 재창출되는 형태, 모든 규제가 제거된 형태로 서비스에 대한 제도가 대부분 개방된 형태 보다 더 진화된 상태로 만성질환자 관리 등에서 활용되고 있다.

2.2. 원격의료의 특징

생활수준의 향상과 고령화로 인한 의료비가 증가함에 따라 질병 예방 및 일상생활 관리의 중요성이 증대되고 있으며 건강 수명 연장을 위한 개인 맞춤형 헬스케어 니즈가 확대되고 있는 상황이다. 헬스케어와 ICT 기술융합의 활용성 증가로 ICT 기술과 헬스케어 산업의 융합을 통해 의료서비스의 효율성이 증대되고 고령화 예방 중심의 관리 및 디지털화에 따라 다양한 비즈니스 모델이 성장하고 있다[4, 5]. 현재 IT 기술의 급속한 발전으로 인해 의료 서비스 산업의 고도화에도 가속도가 붙고 있으며 PACS, EMR, OCS 등과 같은 의료정보 시스템 솔루션들이 병의원 등 의료 기관에 도입되어 있으며, 이를 통해 병의원 업무 효율성을 높여 경쟁력을 높이고 신속한 업무처리로 환자의 의료이용에 따른 편의성을 높이는데 크게 기여하고 있다[6]. 또한 국내외 정부기관들이 다양한 정책을 수립하고 시범사업을 통해 ICT 기술과 헬스케어 산업의 융합을 통해 원격의료서비스를 환자에 맞게 맞춤서비스를 제안하며 다양한 분야에서 예방관리가 가능한 의료 시스템을 기반으로 서비스를 설계하고 있는 것이 현실이다. 현재 이루어지는 원격의료 서비스는 다양한 어플리케이션과 연동되어 언제·어디서나 환자와 의사간 쌍방향 커뮤니케이션이 가능하다. 그러나 민감한 의료 정보를 대상으로 하는 원격의료 데이터 취급에 있어서 언제·어디서나 데이터에 접근한다는 것은 아직까지 보안에 취약하다는 것을 의미한다[6-8]. 스마트 헬스케어[9-10] 원격의료는 환자의 의무기록뿐만 아니라 모든 개인적 임상 데이터에 대한 결과값을 정보화 값으로 전달 받는데 만약 인증 받지 못한 사용자가 환자의 의료 데이터를 악의적인 목적이나 다른 목적으로 사용하기 위해 접근해 데이터를 가져갈 수 있다면 이것은 보안상 심각한 문제가 될 것이다. 따라서 이러한 문제 해결을 위해서는 스마트 헬스케어 원격 의료 서비스에 적합한 안전한 보안 서비스 모델이 필요하다. 또한 안전한 스마트 헬스케어 원격 의료 서비스를 위해 각각의 환자, 보호자, 의사 간호사 등 역할에 맞는 권한의 위임이 발생하게 되고 이를 적절한 키로 대체할 수 있다.

2.3. 모바일 헬스케어와 의료정보 보호

모바일 헬스케어는 홈 케어가 집안 내에서 생체정보를 측정하여 건강관리 서비스를 제공하는 것과 달리, 이동중에도 생체정보를 측정하는 언제·어디서나 건강관리 서비스를 제공하는 기술이다[11,12]. 모바일 헬스케어를 위해서는 이동 중에도 생체정보를 안정적으로 측정할 수 있는 센서 시스템이 필요하며, 이러한 센서 시스템은 착용형 또는 휴대형으로 구현된다. 또한, 측정된 생체정보를 모바일 폰과 같은 휴대용 단말기를 통해 서비스 센터로 전송하도록 구성된다. IBM에서는 모바일 헬스케어와 관련된 일상생활 중 간편하게 혈압, 체중, 심박수, 심전도 등 건강과 관련된 정보를 디바이스를 이용하여 측정하고, 통신 모듈을 통해 전송하여 모바일 헬스케어 서비스를 제공하는 Mobile Wireless Health Solution을 개발하였다[7]. EU에서는 IST(Information Society Technology) Framework Programme을 통해 다양한 형태의 모바일 헬스케어에 대한 연구개발을 추진해 오고 있다[8]. 또한, 최근에는 스마트 모바일 기기를 이용한 다양한 헬스케어 애플리케이션이 개발되고 있다[9]. 의료 정보는 법적으로 민감정보로 분류되는 중요한 정보이며, 반드시 안전하게 전송 및 보관되어야 하므로 본 논문에서도 암호화를 적용하여 안전성을 확보했다[7-9]. 이 논문에서는 다음의 항목들에 대하여 암호화 및 보안을 적용하였다.

① 스마트폰과 헬스케어 단말기 간의 데이터 전송구간
② 스마트폰에서의 데이터 저장
③ 스마트폰과 웹 서버 사이의 전송구간

④ 웹 서버에서의 데이터 저장

Ⅲ. 스마트 헬스케어 서비스를 위한 홍채인식 기반 원격의료 시스템

이 논문에서 만성질환자를 위한 스마트헬스케어를 제공하기 위한 원격의료 시스템을 제안한다.

3.1. 시스템 구성도

현대인들의 식생활의 변화로 만성질환 환자가 급증하고 있다[10]. 그 중 비만은 심혈관질환 및 당뇨병, 고혈압등의 합병증이 발생할 가능성이 높으며, 만성질환은 자기관리의 소홀로 인해 노인성만성질환자에게 큰 고통을 주며, 회복이 불가능한 상태가 초래되고 만성질환자를 예방하거나 관리에는 한계가 있다. 그 중 에서도 만성질환자의 식사 섭취량 및 적절한 식이관리가 중요하며 기존의 처방 방법은 24시간 회상법을 이용하여 하루에 섭취한 식사를 직접 식사일지에 기록하여 병원에 제출한 후 영양사에 의해 처방이 이루어지므로, 만성질환자는 섭취하는 식품의 영양소량을 바로 알기는 어려운 실정이다[10]. 그림 1은 제안하는 스마트헬스케어 서비슬 위한 안전한 원격의료 시스템의 구성도이다. 제안 방식에서는 그림과 같이 환자단계, 헬스케어센터, 서비스 단계로 구분된다.

3.2. 서비스 모델

멀티플랫폼 기반의 헬스 서비스를 제공하기 위해서는 기존의 단일 플랫폼이 아닌 모바일, 웹을 통해 멀티플랫폼 기반으로 제공해야 한다. 만성질환자는 행동수정 프로그램을 실시하며 모바일과 웹을 통해서 Healthcare Center에 서비스 요청하고 다양한 서비스를 제공 받는다. Healthcare Center는 만성질환자의 식이패턴과 행동패턴 데이터를 CDMP(Chronic Disease Multi Platform)를 통해 Healthcare Center로 전달받으며, 각 디바이스의 인터페이스를 관리한다. 서비스는 외부 콘텐츠 정보 제공자를 통해 환자에게 서비스를 제공한다. 외부 콘텐츠 제공자의 식단과 운동 프로그램과 여러 건강관련 DB를 수집하여 의사와 간호사는 CDS 어플리케이션을 통해 만성질환자에게 맞춤화된 운동, 식단을 결정한다. 또한 환자에게 적합한 식당 및 메뉴, 운동센터 등을 GPS와 GIS정보를 통해 웹과 스마트 모바일로 서비스를 제공한다. 서비스 모델을 통해 만성질환자에게 운동과 식단을 처방을 제공한다.

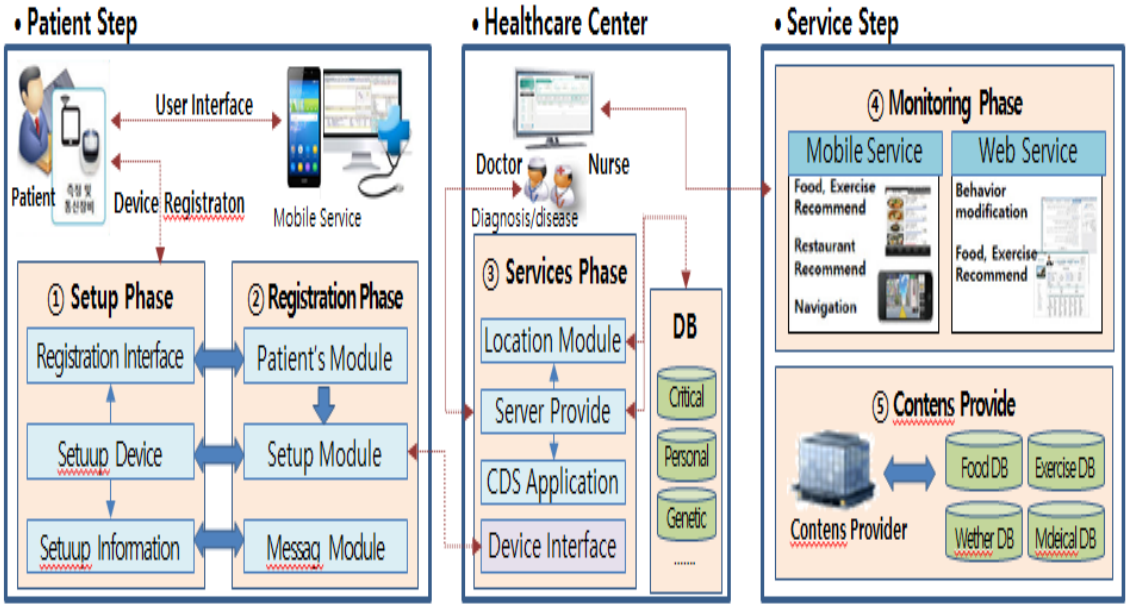


Fig. 1 Integrated framework for Iris-based Authentication in remote medical System

일반적으로 만성질환자의 경우 병원을 방문하여 진단을 받는다. 간호사는 만성질환자의 정보와 임상 평가를 입력하며, 의사는 임상 결과에 대한 식이, 운동 처방을 내린다. 처방이 완료된 후, 만성질환자는 스마트폰을 통해, 식단과 운동을 추천받으며, GPS, GIS등을 활용한 서비스를 제공받는다. 이후 웹을 통해 처방전 확인과 식이/운동 기록, 측정 모니터링이 가능하다. 만성질환자에게 서비스를 제공하기 위해서는 처방 프로세스가 필요하며 그림 2는 만성질환자에게 모바일, 웹 서비스를 제공하기 위한 과정이다. 그림 3의 서비스 흐름도에서 간호사 측에서 확인 및 평가 받은 환자등록 정보와 진료접수 정보를 통해 비만, 당뇨 그 외 만성질환자를 대상으로 환자에게 알맞은 약물과 시술처방을 제공하고, 식이처방전과 운동처방전, Vital 측정결과지 출력 인쇄는 물론, 1주일 단위의 식단 프로그램과 운동 프로그램, 행동수정요법 등을 처방한다. 특히, 식단 프로그램에서는 일반식과 유동식, 죽식, 연식을 구분하여 환자 상태에 따라 칼로리 조절과 영양성분 강화 및 특이체질을 감안하여 환자별 맞춤 프로그램을 제공하고 운동프로그램에서는 환자의 운동 능력과 적응력을 판단하여 유산소, 근력 강화 운동 종목에 대해 식단과 동일하게 맞춤 프로그램을 제공할 수 있다. 또한 처방된 식단과 운동프로그램의 수행 여부에 따른 종합적인 통계분석 자료를 실시간 확인할 수 있다.

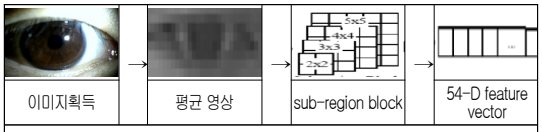
3.3. 안전한 메디컬 정보 보안을 위한 인증

원격진료 환경에서 사용자인증과 원격진료 서비스에서 사용자의 질환에 관련된 의료 서비스를 제공하기 위해서는 본인 인증은 매우 중요한 요소 중 하나이다. 따라서 제안 논문에서 원격진료에서 사용편의성을 고려한 본인 인증 기법을 생체정보를 이용해 강화된 본인 인증을 제공한다. 인증을 위한 구성요소로는 그림 3의 환자 등록단계에서 환자의 홍채를 등록한다. 안전한 메디컬 정보보안을 위한 인증단계는 2단계로 구성된다.

첫 번째 단계에서는 사용자의 홍채를 사용 중인 디바이스를 이용해 등록하고 원격의료 디바이스에서 생체정보를 인증한다.

두 번째 단계로는 원격의료 디바이스는 메디컬센터에 사용자 인증과 디바이스인증을 통해 메디컬 정보를 헬스케어 센터로 전달한다.

그림 2는 스마트디바이스를 이용해 획득한 홍채영상에서 만성질환자에 질병에 대한 특징점을 추출하기 위해 홍채영상의 질병 특징점 추출을 위한 전처리 알고리즘이다.




```
/// RGB색공간 이미지에서 sobel 및 laplacian 필터처리
/// </summary>
/// <param name="input"></param>
private void processRGB(Mat input)
{
    Mat copy_Original = input;
    Cv2.Resize(copy_Original, copy_Original, new
      OpenCvSharp.CPlusPlus.Size(365, 318));
    Mat gray = new Mat();
    Cv2.CvtColor(copy_Original, gray, ColorConversion.RgbToGray);

    Mat laplacian = new Mat();
    Mat sobel = new Mat();

    Cv2.Laplacian(gray, laplacian, MatType.CV_8U);
    pictureBoxIpl1.Image = ChangeM2B(laplacian);
    pictureBoxIpl1.SizeMode = PictureBoxSizeMode.StretchImage;
    sobel = SobelFilter(gray);
    pictureBoxIpl2.Image = ChangeM2B(sobel);
    pictureBoxIpl2.SizeMode = PictureBoxSizeMode.StretchImage;
    Mat edge = new Mat();
    Cv2.Canny(sobel, edge, 120, 255, 3);
    using (new Window("sobeltoedge", edge))
    {
        Cv2.WaitKey();
    }
    houghtrans(edge);

}//end of Method
```

Fig. 2 Feature point extraction algorithm

제안 논문에서는 안전한 원격진료를 위한 2단계 인증을 통해 보안 요구사항 중 기밀성과 무결성을 보장하기 위해 사용자의 건강과 의료서비스를 제공하기 때문에 사용자 인증에 오류가 발생할 경우 치명적인 의료문제를 발생시킬 수 있다. 또한 기존의 패스워드 방식 및 공개키 기반의 사용자 인증기법은 비밀번호를 입력해야하는 불편함을 가지고 있어 만성질환자들에게는 부적절하다. 따라서 제안 논문에서는 생체정보를 이용해 사용자인증을 수행함으로 사용자들에게 편의성을 제공한다. 사용자의 생체정보 인식이 완료되면 환자 단말기를 이용해 메디컬센터에 접속하기 위한 사용자 메타데이터 기반의 인증 방식을 제공한다. 환자 단말기에 안전하게 저장되어 있는 환자 메타데이터 안에 인증키(AK)를 기반으로 식별 및 인증 서비스를 제공한다. 원격의료 환경에서 사용자 단말기는 메디컬 헬스센터에 등록되어 있다. 사용자 인증 및 사용자 단말기 인증을

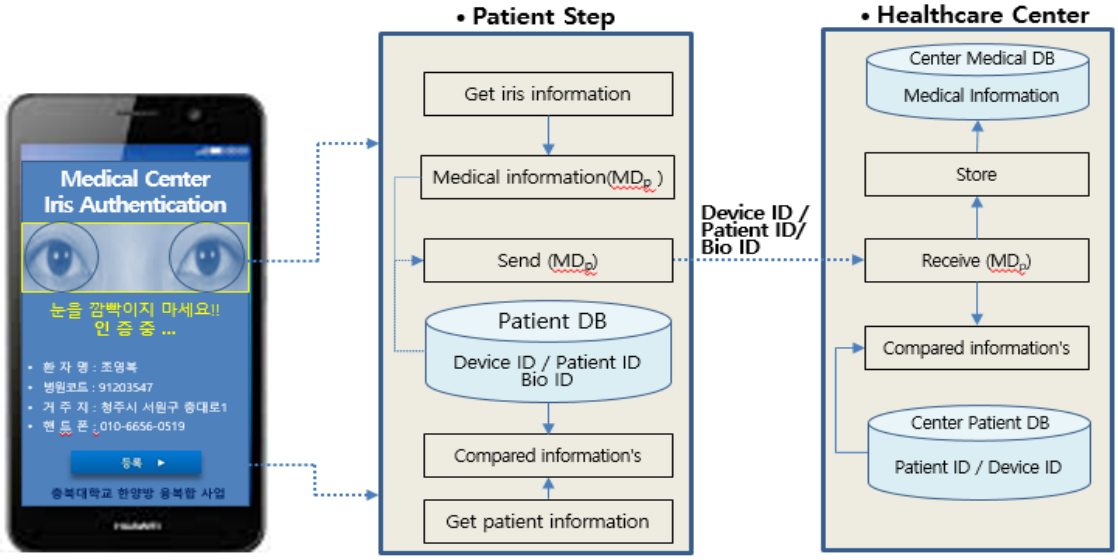


Fig. 3 Iris-based Authentication Protocol

위한 인증 값 (AK)를 통해 이루어진다. 모바일 단말기를 이용한 안전한 원격진료를 제공하기위해 제안 논문에서는 ECC기반의 키 교환 암호 알고리즘을 사용한다. 사용자 단말기와 메디컬 센터는 공개키 쌍을 생성하고 생성된 공개키 정보를 상호 교환해 마스터키(k_m)을 생성한다. 사용자단말기에 적용되는 공개키 생성 메커니즘은 제약된 환경을 고려해 한번 생성한 키를 지속적으로 사용한다. 또한 메디컬 센터는 사용자단말기가 접속할 때 마다 사용되는 키를 임의의 난수를 이용해 세션키를 생성하고 사용한다. 제안 논문의 키 관리 프로토콜은 다음과 같다.

① 사용자 단말기는 공개키 쌍을 생성하여 개인키, 공개키, 키 쌍 생성 인자를 구성한다. 각 사용자 단말기는 통신에 사용할 키를 생성하고 개인키는 시스템에 저장한다.

$$M(SK_{PD}, PK_{PD}, D_{pm})$$

② 생성된 공개키와 키 생성 인자(PK_{PD}, D_{pm})를 메디컬센터로 전달한다.

③ 메디컬센터는 사용자단말기로부터 송신한 키 생성인자(PK_{PD}, D_{pm})에서 공개키는 저장하고 키 생성 인자를 이용해서 공개키 쌍을 생성한다. 또한 메디컬 센터는 개인키, 공개키, 키 생성 인자인 (SK_{PD}, PK_{PD}, D_{pm})를 생성 후 개인키는 메디컬 센터에 안전하게 보관한다.

④ 메디컬센터에서 생성된 공개키(PK_{PD})를 사용자 단말기로 전송한다.

⑤ 사용자 단말기는 송수신 키 정보를 기반으로 마스터키(MK)를 생성한다.

⑥ 메디컬센터는 송수신 키 정보를 이용해 마스터키(MK)를 생성한다.

3.3.1. 안전한 메디컬 정보보안 인증프로토콜

환자가 사용하는 단말기와 메디컬 센터의 인증프로토콜은 다음과 같다.

① 환자 단말기와 메디컬 센터의 인증을 위한 정보교환은 CC암호화 기반의 DH 키 교환 프로토콜을 통해서 공유된 암호 키로 안하게 송수신한다.

② ECC암호화 기반의 DH 키 교환 프로토콜을 통해 환자 단말 기는 Master Key를 생성한다.

③ ECDH 암호 키 교환 프로토콜을 통해 메디컬 센터는 Master Key를 생성한다.

④ 환자 단말기는 메디컬 센터 연결하는 경우 바이오 인증을 완료한 사용자의 식별정보와 해당 환자단말기의 Auth Key를 기반으로 Max_Counter 보다 작은 임의의 값을 인자로 해서 인증 값(AV)를 생성한 값

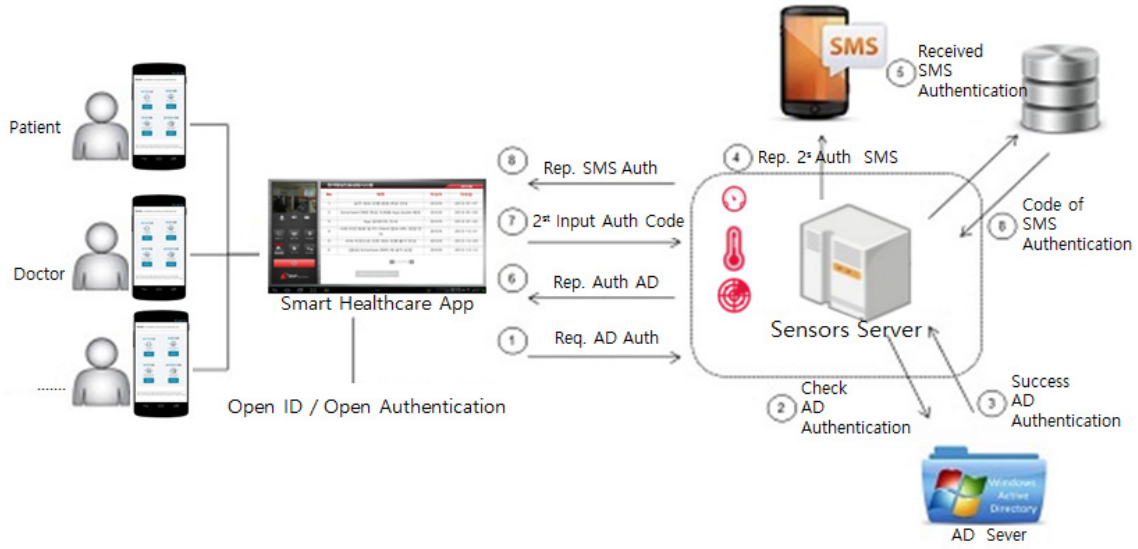


Fig. 4 Proposed Secure System Structure

은 전송한다.

$$E[ID, H_{RC}(value), RC]K_{master}$$

⑤ 메디컬 센터는 수신한 값을 E_{master}를 이용해 복호화한 후 해당 ID를 획득한다. 사용자 정보DB에 저장된 인증 값과 수신한 값을 단방향 함수를 이용해 일치 여부를 검증한다.

$$[H_{RC(value)}? = H_{mRCr}(H_{RC}(value))]$$

⑥ 사용자 단말기의 인증이 완료되면 메디컬센터의 접근을 허용한다.

Ⅳ. 제안시스템의 안전성 평가

제안 논문에서는 안전한 원격진료 인증 프로토콜을 사용한 앱 구동과 관리자페이지 실행 화면을 그림 4와 같이 실행하였다. 제안 논문에서는 사용자 인증 및 원격진료 인증 프로토콜에 사용되는 환자단말기에 대한 사용자의 생체정보를 이용한 사용자(환자)단말기와 메디컬 센터 인증을 1차 수행한다. 1차 인증 후 2단계 인증절차로 의료 환경을 고려한 사용자의 본인확인을 강화하고 인증방식을 경량화 하여 실시간 제공이 가능하도록 제안하였다. 또한 원격의료의 특성상 안전하고 신뢰성이 보장되지 않은 네트워크상에서의 사용자 식별 및 인증정보를 매번 생성하여 사용하는 일회용 인증정보를 활용해 안전성을 확보하였고 스마트폰의 네트워크 자원 제약을 고려한 최소한의 자원을 할당하는 효율적인 알고리즘을 사용하였다.

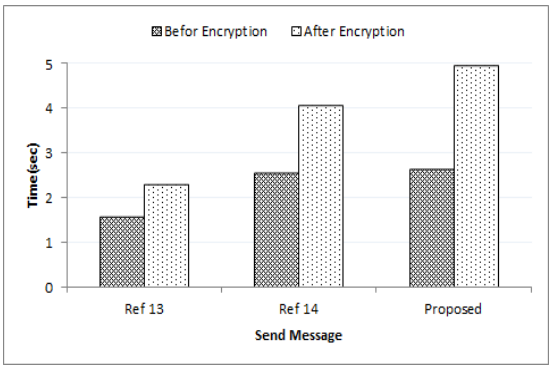


Fig. 5 Encryption strength comparison

제안논문에서 사용자 단말기는 홈 네트워크와 연결되어 사용자 인증으로 아이디와 패스워드 또는 생체정보 인증방식을 제공한다. 또한 홍채인식을 위한 단말기의 카메라는 사용자의 편의성과 개인 식별의 강화로 기존 아이디와 패스워드 방식보다 빠른 인증속도와 높은 보안강도를 제공한다. 제안방식의 안전성평가를 위해

그림 5는 암호화 강도를 기존 방식과 비교한 결과이다. 환자데이터베이스는 사용자 단말기에서 관리되며 단말기 식별정보와 사용자 식별정도, 생체인식정보를 저장하고 있고 단말기 인증정보인 MAC, 제품일련번호, 사용자 식별정보로 아이디와 패스워드를 사용한다. 생체인식정보로는 홍채인식 레퍼런스를 저장함으로 강력한 사용자 인증에 활용된다. 메디컬 센터는 사용자 단말기와 인증을 수행하고 전송된 메디컬의료정보를 저장한 후 기존의 정보와 함께 분석을 수행해 만성질환자들의 종합적인 건강상태를 확인한 후 처방 및 조치를 환자에게 전달한다. 만약 환자에게 이사이증후가 발생되는 경우 환자와 오프라인으로 연락을 수행하고 응급처리 프로세스를 수행한다. 메디컬정보 DB는 메디컬 센터 내에 사용자의 건강 의료정보를 이력별로 저장하고 관리함으로 사용자의 종합건강정보를 분석하도록 제공한다. 표 2는 제안 알고리즘의 보안 기법 평가표로 데이터의 안전성, 기밀성, 무결성 및 프라이버시가 제공됨을 나타낸다.

Table. 2 The evaluation of proposed security technique

Evaluation items	Our Algorithm
Data Security	Offer
Data Confidentiality	Offer
Data Integrity	Offer
Privacy	Protect

Ⅴ. 결 론

스마트 헬스케어 서비스를 위한 안전한 원격진료에서 사용자 인증은 환자, 의사, 간호사, 관련기관 담당자 등 사용자의 정보 및 사생활 침해를 막고 정확한 의료정보의 전달을 위해 생체 정보를 사용하는 사례가 증가하고 있다[13][14]. 이는 생체정보가 타인에게 노출되거나 분실하는 경우에도 기존 비밀번호나 아이디처럼 사용자 정보를 쉽게 변경하거나 악용하기 어렵다는 장점을 갖는다. 따라서 이 논문에서는 안전한 스마트 헬스케어 서비스를 위한 원격진료에 생체정보 즉 홍채의료정보를 이용한 인증을 기반으로 개인 프라이버시 보호와 통신상 전달되는 데이터의 무결성과 기밀성을 보장한다. 또한 원격의료가 대두되는 시점에서 안전한 원격의료 시스템 모델을 정의하고 2단계 인증프로토콜을 통해 사용자의 개인정보를 보호하고 또한 높은 보안능력을 갖는 고성능의 개인인증용 생체정보 시스템 모델을 제시하였다.

노인성 만성질환 환자들을 위한 원격의료 시스템으로 기존 ID/PW방식보다 편리하면서 안전한 인증방식을 제공한다. 노인성만성질환자의 사용 편의성과 의료환경의 특수성을 고려했을 경우 제안방식은 적합한 인증수단으로 타인에게 도용되거나 분실시 쉽게 변경하기 어려워 기존 ID/PW방식에 비해 안전하다. 또한 스마트헬스케어서비스를 위한 원격의료 시스템은 의료정보 및 헬스케어 정보의 민감한 프라이버시 유형중 하나로 원격의료 시스템에서 매우 중요한 보안요구사항 중 하나이다. 따라서 우리는 제안 논문에서 민감한 의료정보 및 개인정보 보호를 제공하는 2단계 인증 프로토콜을 제시하였다. 제안 방식은 기존 ID/PW방식보다 높은 기밀성과 무결성을 제공하며 보다 강력한 안전성을 제공함을 증명하였다.

ACKNOWLEDGMENTS

This work (No.C0422615) was supported by Business for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Small and Medium Business Administration in 2016 and and This research was supported by the CHUNGBUK TECHNOPARK, Korea, under the (2016한양방융복합) support program (2016070793) supervised by the NIPA(National IT Industry Promotion Agency)

REFERENCES

[1] J. Y Oh, “Medical information trand,” National Information Society Agency, NCA CIO REPORT, vol. 5, no.11, 2006.

[2] Valerie S. Prater, “Confidentiality, privacy and security of health information: Balancing interests,” *Article of Biomedical and Health Information Sciences*, pp.4. Dec.

2014.

[3] J. C. Nam, W. K. Seo, J. S. Ba, Y. J. Jo, “Design and Development of Personal Healthcare System Based on IEEE 11073/HL7 Standards Using Smartphone,” *The Journal of Korean Institute of Communications and Information Sciences*, vol. 36, no.12, pp.11-12, Dec. 2011.

[4] J. E, Song, S, H, Kim, M, A, Jeong, K. I, Jeong, “Security Issues and Its Technology Trends in u-Healthcare,” *The Journal of Electronics and telecommunications trends*, vol. 22, no. 1, pp. 119-129, Jan. 2013.

[5] M. Tentori, J. Favela and M. D. Rodriguez, “Privacy-Aware Autonomous Agents for Pervasive Healthcare,” *The Journal of IEEE Intelligent Systems*, vol. 21, no. 6, pp.55-62, Jan. 2007.

[6] J. H. Park, B.T,G Hwang, “Health IT Technology Trends,” *The Journal of Korean Institute of Communications and Information Sciences*, vol. 28, no. 5, pp.21-27, May 2011.

[7] J. Sun and Y. Fang, “Cross-Domain Data Sharing in Distributed Electronic Health Record System,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 6, pp.754-764, June 2010.

[8] Article 18, the 23 of the Privacy Act and the Personal Information Protection Act , pp.1-41, Mar. 2011.

[9] S. H. Lee, S. S. Yoo, “The status and outlook of mobile healthcare application,” *The Journal of ICT & Media Policy*, vol.26, no.7, pp. 1-23, June 2014.

[10] Y. H. Lee, J.H. Kim, J.K. Kim, K.P. Min, “Smart Phone based Personalized Menu Management System for Diabetes Patient,” *The Journal of the Korea Contents Association*, vol. 10, no. 12, pp. 1-9, Oct. 2010.

[11] H. S. Park, H. Cho, & H. S.Kim, “Development of cell phone application for blood glucose self-monitoring based on ISO/IEEE 11073 and HL7 CCD,” *The Journal of Healthcare Informatics Researc*, vol. 21, no. 2, pp. 83-94, Apr. 2015.

[12] H. S. Park, “Development of m-Health application based on Medical informatics standards,” *Journal of Korea Multimedia Society*, vol. 17, no. 5 pp. 640-653, May 2014.

[13] S. C. Noh, E. J. Song, “A Study of Smart Healthcare Services Software Quality Satisfaction Rating System based on QoS(Quality of Service) Measurement Model”, *The Journal of the Korea Institute of Information and Communication Engineering*, vol. 18, no. 1, pp. 149-154, Jan. 2014.

[14] Y.B Cho, S. H. Woo, S. H. Lee, J. B. Pack, “A Secure Telemedicaine System in Smart Health Environment using BYOD”, *Journal of the Korea Institute of Information and Communication Engineering*, vol. 19, no. 10, pp. 2473-2480, Oct. 2015.

조영복(Young-Bok Cho)

2005: 충북대학교 전자계산학과 공학석사.
2012: 충북대학교 전자계산학과 공학박사
2016: 충북대학교 의학과 박사과정수료
현 재: 충북대학교 초빙교수
※관심분야: 의료영상처리, 정보보안, 의료정보보호
Email : bogicho@cbnu.ac.kr

우성희(Sung-Hee Woo)

1993: 충북대학교 전자계산학과 이학석사.
1999: 충북대학교 전자계산학과 이학박사
현 재: 한국교통대학교 의료정보공학과 교수
※ 관심분야: 침입차단 및 방지, 의료정보보호, 정보보안, 컴퓨터네트워크
Email : shwoo@ut.ac.kr

이상호(Sang-Ho Lee)

1989: 숭실대학교 전자계산학과 공학박사.
현 재: 충북대학교 소프트웨어학과 교수
※관심분야: 컴퓨터네트워크, 정보보호, 데이터통신
Email : shlee@cbnu.ac.kr

김민경(Min-Ho Kim)

2006: 연세대학교 보건학석사
2016: 충북대학교 의학과 박사과정 수료
현 재: 협성대학교 겸임교수
※관심분야: 건강증진, 빅데이터
Email : tomarow@hanmail.net