유비쿼터스 헬스케어를 위한 전자지불 시나리오

홍인식* · 백장미**

1. 서 론

최근 인터넷의 급성장에 따라 유선망을 비롯하여 무선 네트워크 망 기반의 다양한 서비스가 소개되고 있다. 특히, 유선과 무선의 통합 환경이 제시되면서 유비쿼터스 환경이라는 용어가 등장하고 있다. 유비쿼터스 환경이란 언제 어디서나 네트워크에 접속할 수 있는 환경으로서 모든 사물과 사람이 보이지 않는 네트워크로 연결되어 언제나 접속이 가능하고 언제나 상호작용이 가능한 것을 의미한다. 유비쿼터스는 사용자 중심의 서비스를 제공하는 것을 목적으로 하고 있기 때문에 다양한 인터넷 비즈니스 모델과의 접목으로 가치창출에 대한 가능성이 높은 분야이다. 개인의 삶의 질과 관련되어 건강과 가장 밀접한 관계가 있는 헬스케어 서비스 분야에서 유비쿼터스 비즈니스 모델의 개발이 활발히 이루어지고 있다. 기존의 단순한 모니터링 기능에 한정된 헬스케어 서비스를 모바일 단말기를 중심으로 다양한 네트워크 망을 이용한 어플리케이션의 개발이 활발히 진행 중에 있다. 따라서 본 논문은 다양한 유비쿼터스 네트워크 환경 중에서 모바일 단말기와 USIM(Universal Subscriber Identity Module)을 이용하여, 유비쿼터스 시대에 맞는 헬스케어 서비스의 한 분야로서 원격 병원 진료 서비스와 지불 프로토콜을 제안하고자 한다. 본 제안 방식은 모바일 단말기와 USIM, 네트워크 망의 연계를 통하여 기존의 진료 시스템 보다 효율적인 진료 시스템을 연구한다. 제안방식의 경우 일반적인 유비쿼터스 환경에 맞는 병원 진료 시스템을 구성하기 위해서 개개인의 정보를 수시로 체크하고 전송하기 위한 기술이 필요하며, 진료 및 지불에 관련된 데이터는 인증이 필수적으로 요구되므로 안전하게 데이터를 전송하고 인증할 수 있는 프로토콜을 추가적으로 제시하였다. 따라서 본 논문의 2장에서는 헬스케어의 개념과 과거의 헬스케어와 유비쿼터스 상에서의 헬스케어 시스템을 비교 분석하고, 3장에서 헬스케어 시스템 상에서 필요한 보안사항을 분석한다. 4장에서는 분석된 보안사항을 기반으로 모바일 단말기를 이용한 병원 진료 시스템을 구성하고 지불 프로토콜을 제안하고 분석한 뒤 5장에서 결론을 맺도록 한다.

본 연구는 2002년도 순천향대학교 학술연구조성비 과제로 지원받아 수행하였음.

* 순천향대학교 공과대학 정보기술학부 부교수
** 순천향대학교 대학원 전산학과 석사과정

2. 유비쿼터스 헬스케어

일반적으로 헬스케어란 예방, 치료, 질병관리, 정신적 육체적인 안정유지 등의 건강과 관련된 서비스를 제공하고 관리하는 것을 의미한다. 헬스케어는 3세대로 구분하여 설명할 수 있다. 1세대는 독립적인 헬스케어 형태로서 사용자가 오프라

인으로 병원을 통해서만 헬스케어 서비스를 이용할 수 있었으며 의사의 진단과 치료 및 의료기구에 의존적인 형태였다. 그러나 인터넷 보급의 확산으로 텔레 포털 병원과 같은 디지털 화된 헬스 서비스 등의 다양한 전산 시스템이 구비되면서 환자의 병을 초기에 발견하고 진단할 수 있게 되었으며, 환자의 데이터를 전자적으로 관리하게 되었다. 더 나아가서 현재는 다양한 네트워크를 기반으로 하여 분산된 환경에서의 헬스케어 서비스를 제공하려고 연구 중이다. 특히, 모바일 단말기 및 다양한 센서 칩을 이용한 환자의 지속적인 모니터링 시스템을 통하여 셀프케어 및 연속적인 헬스케어 서비스를 제공할 수 있으며, 위급한 상황을 신속하게 대처할 수 있도록 인공지능적인 헬스케어 서비스를 제공하게 될 것이다. 유비쿼터스 헬스케어는 환자가 직접적으로 느낄 수는 없지만, 환자의 상태를 판단하여 물리적 환경을 통해 헬스 서비스 제공하게 된다. 이렇게 헬스케어를 위한 서비스도 변화하는 이유는 전 세계적으로 보다 낳은 헬스케어 서비스를 원하고 있고, 질 높은 건강 데이터의 관리를 요구하고 있기 때문이다. 그림 1은 유비쿼터스 환경에서 헬스케어를 위한 전반적인 기반 환경을 보여주고 있다.

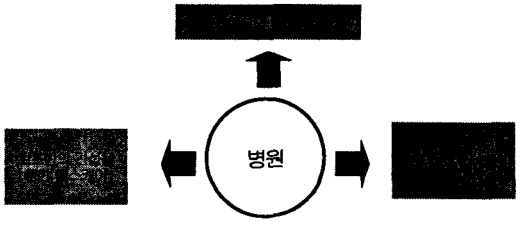

그림 1. 유비쿼터스 헬스케어

3. 헬스케어 서비스를 위한 보안 요구사항

모바일 헬스케어 서비스의 경우 정당한 서비스 요구자에게 환자의 건강 정보를 전송하여 지속적인 모니터링이나 응급사항이 발생되었을 시 신속한 대처나 빠른 조치를 취하기 위한 부가가치 서비스이다. 그러나 이는 사용자의 개인정보와 매우 밀접한 관계가 있으며, 이에 대한 보안 서비스가 제공되지 않을 경우 악의적인 사용자에 의해 정당한 사용자의 프라이버시 정보가 악용될 수 있다. 따라서 모바일 헬스케어 서비스를 제공하기 위해서는 다음과 같은 보안 사항이 요구되며, 이는 다음과 같다.

3.1 기밀성과 인증

기밀성은 보안상에서 기본적으로 제공되어야 하는 요소로서 모바일 헬스케어 상에서의 데이터 전송 및 핸들링 사이에서 필요하다. 데이터는 데이터의 권한이 있는 사람만이 접근이 이루어져야 한다. 헬스케어를 위한 병원 진료 서비스는 환자가 병원을 예약하고 진료를 받고 처방을 받는 등의 모든 절차를 위하여 환자의 데이터를 필요로 한다. 그러나 환자의 데이터는 환자의 개인 정보 및 의료에 관련된 모든 정보를 내포하고 있으므로 개인의 프라이버시와 밀접한 관련성이 있다. 본 논문에서 제시하는 시나리오는 모바일 단말기 및 PDA를 이용한 헬스케어 시스템이기 때문에 모바일 단말기의 SMS서비스 제공 시 어떤 방식으로 인증을 할 것이며, 안전하게 데이터를 전송할 것인지에 대한 연구를 수행한다. 따라서 사용자의 프라이버시 정보에 대한 기밀성 보장을 위해서는 프라이버시 보호 서비스가 보장되어야 한다. 또한 전송 데이터에 대한 인증과 기밀성 뿐만 아니라 사용자에 대한 인증 서비스 제공을 위한 연구를 추가적으로 수행하고자 한다.

3.2 무결성

무결성은 데이터가 전송되는 동안 데이터의 위

조나 변조가 발생되지 않는 것을 의미한다. 병원 진료 서비스는 정확한 환자의 정보를 통해서 환자를 진료하고 처방을 내릴 수 있다. 환자의 데이터가 위조되거나 변조되었다면 환자에게 치명적인 결과를 초래할 수도 있기 때문이다. 따라서 병원 진료 시스템 상에서의 무결성은 제공되어야만 한다.

3.3 유용성

유비쿼터스 상에서의 모든 비즈니스 모델은 인간 중심의 시나리오를 제시하고 있다. 헬스케어 상에서의 모든 시나리오 역시 인간 중심적이어야 한다. 즉, 어떠한 권한을 가진 사람이라면 언제 어디서나 데이터의 접근이 가능해야 하고 손쉽게 자원을 이용할 수 있어야 한다. 즉, 실제적으로 서비스를 제공하는 시스템에 문제점이 발생하더라고 사용자는 실제로 서비스 상에서의 문제점이 발생하였다는 것은 인지하지 못하도록 시스템을 구성해야 한다.

4. 헬스케어를 위한 원격 병원 시나리오

본 장에서는 유비쿼터스 상에서 요구하는 다양한 비즈니스 모델 중 헬스케어와 관련된 원격 병원 시스템을 제안하고 설명하고자 한다. 특히 병원 진료 후의 안전한 지불에 대한 프로토콜을 제시한다. 사용자나 환자는 모바일 단말기를 통해 예약 및 지불을 수행할 수 있으며 지불 수행은 USIM을 이용하여 지불하거나 네트워크 화폐를 통해 지불하는 프로토콜을 제안한다. 진료에 대한 지불을 위하여 병원을 예약하는 과정부터 진료, 진료후의 지불과정사이에서 전송되는 데이터의 안전성을 위한 프로토콜을 제시한다.

4.1 전체 구성도

유비쿼터스 환경에서는 다양한 헬스케어 모델이 구성될 수 있다. 본 논문은 다양한 비즈니스 모델이 가능하다고 가정하고 사용자가 모바일 단말기를 이용하여 헬스 서비스를 받는 경우에 초점을 두었다. 따라서 전체 구성도는 여러 가지 시나리오가 가능한 구성도를 설명한다. 전체 구성도를 소개한 후 병원 시스템의 지불에 초점을 두어 지불 프로토콜을 제안하도록 한다.

유비쿼터스는 다양한 기기로의 네트워크 접근을 가능하게 하는 환경이므로, 본 시스템은 일반적인 PC 환경과 모바일 단말기를 이용한 환경, 센서 네트워크 환경을 제시한다. 즉, 병원과 약국은 PC나 단말기 중심의 환경을 구축하고 있으며, 사용자는 다양한 무선 바이오센서 네트워크와 모바일 단말기를 기반으로 한 환경으로 이루어져 있다. 본 연구는 다양하게 제시되는 시나리오 중에 사용자 환경을 무선 네트워크 환경으로 가정하고 프로토콜을 제시한다.

즉, 사용자(환자)는 무선 단말기로 사용할 수 있는 PDA나 모바일 폰을 이용하여 병원에 접근할 수 있고 모든 단말기는 개인의 인증 정보의 기밀성 및 무결성을 위하여 USIM을 내장한다. 사용자 또는 환자는 모바일 단말기 및 다양한 센서를 통하여 환자의 상태를 체크한다. 즉 사용자는 USIM이 내장된 모바일 단말기를 이용하여 헬스케어 서비스를 제공받을 수 있고, 다양한 센서 네트워크 장비를 통하여 환자의 상태를 체크하고 이상이 발생하였을 경우 이상 여부를 병원이나 의사에게 전달하는 서비스를 제공받을 수 있다.

병원 역시 다양한 단말 장치를 이용하여 환자의 상태를 모니터링 할 수 있으며 다양한 네트워크 장비는 환자와 병원 사이에 예약, 진료, 지불과 관련된 다양한 서비스를 제공받을 수 있도록 도와준다. 병원은 또한 신뢰할 수 있는 기관으로서 의료보험 관리 공단과 연계되어 사후 지불이나 진료 및 처방에 대한 인증 여부를 확인 할 수 있다. 그림 2는

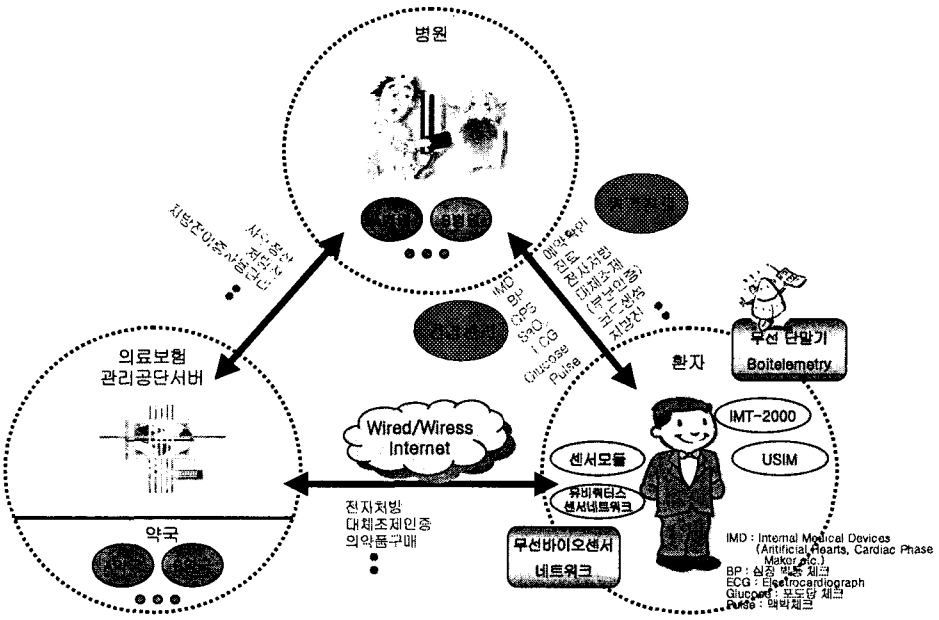

그림 2. 전체 구성도

다양한 시나리오를 제시할 수 있는 유비쿼터스 환경에서의 헬스케어 시스템의 구성도를 보여주고 있다.

본 논문에서는 사용자의 무선 단말기와 연계되어 있는 USIM이 중요한 역할을 제공한다. 사용자는 단말기의 USIM을 사용하여 진료 기관의 선택할 수 있고 진료 기관 예약할 수 있으며, 자신의 병력 정보 조회 및 진료, 투약, 주사 과정에서의 환자 인증, 병원비 지불 등의 문제를 해결할 수 있다. 특정 병원의 진료 예약을 하기 위해서는 사용자는 이동 통신 단말기를 이용하여 무선 인터넷으로 의료 통합 서버에 접근한다. 의료 통합 서버는 USIM에 저장된 사용자의 개인 식별 번호와 인증서를 확인하여 접근 권한을 부여한다. 인증된 사용자는 의료 통합 서버에 코드화 된 병원 중에 하나를 선택하고 예약 접수 과정을 거친다. 진료시에 USIM에 저장된 개인 인증서를 이용하여 진료 기록이 해당 사용자의 데이터베이스에 입력된다. 입력된 내용은 인증된 사용자라면 언제든지 무선 인터넷을 통하여 확인이 가능하다. 진료가 끝나고 주사나 투약 과정에서도 USIM만 있으면 해당되는 내용이 자동으로 단말기에 나타나게 되고 정확한 주사나 투약 서비스를 받을 수 있다. 진료를 받은 후, 약이 필요한 경우, 처방전을 사용자가 지정하는 약국으로 보내는 것이 필요하다. 사용자는 USIM을 가지고 가서 약국 서버 컴퓨터에 무선으로 연결하여 자신의 인증 정보를 보내준다. 그러면 약국 서버 컴퓨터가 네트워크를 이용하여 사용자의 ID를 이용하여 병원의 서버와 접속하여 처방전을 다운로드받는다. 즉, 병원과 약국 서버는 의료보험과 연계된 통합 관리 프로그램을 통해 환자의 USIM 내의 정보를 활용하여 진료와 처방에 적용할 수 있다.

4.2 시스템 구성요소

다음은 유비쿼터스 기반의 전자 지불 시스템을 제안하기 위한 구성 객체에 대해 논의하고자 한다.

4.2.1. 헬스 서비스 제공자(병원)
- 헬스케어 제공자는 건강관리 서비스와 관련된 개체들이 내/외부적인 기능을 제공
- 프로세스 관리 지원
- 작은 프로세스의 조합을 통한 완전한 프로세스 상태 복원
- 활성과 진행의 협력
- 인증
- 신뢰할 수 있는 정보의 제공
- 환자 중심의 지식 프로세싱

4.2.2. 사용자(환자)
- 개인적인 헬스 서비스 요구
- 기동성 있는 서비스의 요구
- 이동성
- 환자 스스로 질병에 대한 정보 제공 요구

4.2.3. 모바일 컴퓨팅(PDA, 모바일 단말기)
- 사용자가 소유하고 있는 단말기의 성능향상을 최대화 하여야함
- 사용자의 개인적인 정보나 작업에 관련된 영역의 적정선을 유지
- 건강관리 시스템의 비밀 부분과 공개 부분을 명확히 관리
- 모든 헬스케어 관련 개체들간의 연관성을 유지
- 환자의 연락처 혹은 환자의 개인 사항과 관련된 키 요소에 대한 관리
- 다양화된 모바일 단말기 제공 환경에서의 서로 상이한 헬스 서비스를 제공하기 위한 적은 대역폭과 같은 요구사항들이 필요
- B2B상에서 헬스케어 분야의 적용을 위한 노력필요

4.3 헬스케어 지불 프로토콜

위에서 제시한 여러 가지 요구사항을 바탕으로 다양하게 제시될 수 있는 헬스케어 서비스 중에서 모바일 단말기를 통한 병원 예약 및 지불 프로토콜을 제안한다. 지불은 USIM을 이용한 지불과 USIM에 지불 데이터가 없는 경우를 위한 네트워크형 지불에 초점을 두어 프로토콜을 제시한다.

4.3.1. USIM과 네트워크형 지불을 제공하는 헬스케어 지불 프로토콜

그림 3은 USIM과 네트워크형 지불을 제공하는 헬스케어 지불 프로토콜이다. 즉 지불하는 화폐 종류와 무관하게 헬스 정보를 제공하는 프로토콜을 설명한다.

그림 3에서 보는바와 같이 모바일 단말기를 통한 헬스케어 지불을 위해서 전체 구성도에서 필요한 요소만을 추출하였다. 병원은 다양한 네트워크 장비로 환경이 구축될 수 있으며 병원의 의사와 간호사는 다양한 단말 장치를 통해 서비스를 지원받는다고 가정한다. 지불 게이트웨이는 신뢰할 수 있는 기관으로서 의료보험 관리 공단이의 역할을 수행한다. 은행은 가상은행으로서 USIM의 화폐를 충전하거나, 네트워크형 지불을 수행할 경우 필요한 요소이다. 본 그림은 병원을 선택하고 예약하여 진료를 받고 진료후의 지불에 관련된 프로토콜이다. 즉 진료 후의 약국이나 다른 처방에 관한 사항들은 배제하였다. 사용자는 모바일 단말기를 통하여 병원을 예약한다. 병원을 예약하기 위해서 사용자의 ID와 인증코드에 사용자의 서명이 된 데이터를 병원으로 전송한다. 병원은 사용자의 데이터를 확인하고 병원 예약 시간과 담당의사 ID등의 정보에 병원의 서명이 포함된 데이터를 사용자에게 전송한다. 사용자는 나중에 일어날 지불을 위하여 지불게이트웨이와 지불초기화 과정을 수행하고 병원과 지불게이트웨이 사이에서는 지불 초기화에 대한 검증이 발생한다. 다시 한번 병원은 예약 검증 완료 데이터를 사용자에게 보내주고 사용자는 병원을 방문하거나, 병원의 담당의

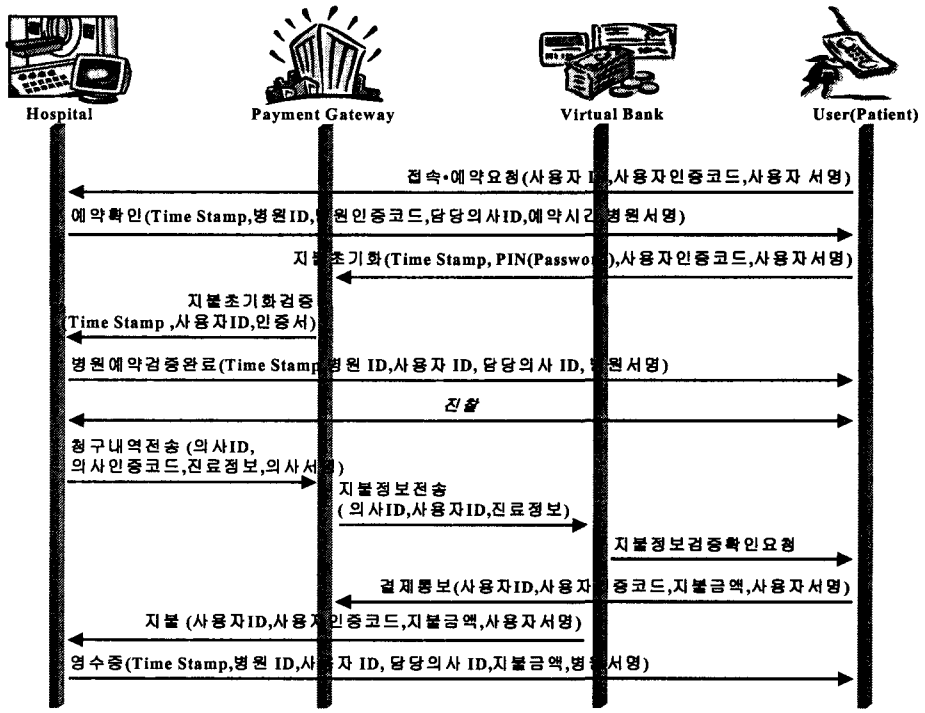

그림 3. USIM과 네트워크형 지불을 제공하는 헬스케어 지불 프로토콜

사가 사용자를 찾아오거나 등의 과정을 통해서 진찰을 받게 된다. 진찰이 완료되면 의사는 진찰과 주사 등의 처방에 관련된 청구 내역을 요구한다. 이 때 보내지는 정보는 의사의 서명을 통해서 전송되며 사용자는 청구 내역을 확인하고 지불을 수행한다. 병원의 서명을 통하여 데이터를 보낼 수도 있지만 의사의 서명을 통해서 잘못된 처방이 발생하였을 경우 등의 상황을 위한 부인봉쇄의 기능을 할 수 있다. 지불이 완료되면 병원 측은 사용자에게 영수증을 전송한다.

4.3.2. USIM을 통한 헬스케어 지불 프로토콜

그림 3에서 제시한 프로토콜은 지불방법에 관련 없이 제시된 모바일 지불 프로토콜 모델이다. 그림 4는 USIM을 이용한 지불에 초점을 맞춘 프로토콜을 보여주고 있다.

그림 4에서 보는바와 같이 USIM을 이용하여 지불을 수행하는 프로토콜은 가상은행을 포함시키지 않았다. USIM 내의 화폐는 이미 은행을 통해서 충전되어 있다고 가정하였고 USIM에서 제공하는 암호화 기법을 통해서 안전하게 데이터를 저장하고 있기 때문에 은행은 그림에서 설계하지 않았다. 그림 3에서 제시한 프로콜과 마찬가지로 USIM에 내장되어 있는 사용자 정보를 통해서 병원의 예약과 지불을 수행하게 된다.

4.3.3. 네트워크형 지불을 수행하는 헬스케어 지불 프로토콜

그림 5는 모든 데이터 전송 및 인증을 위해서는 USIM에 내장된 데이터를 사용하지만 최종적으로 지불을 수행할 때 USIM 내의 지불 데이터를 이용하는 것이 아니라 은행의 네트워크형 전자화폐를 이용하는 경우를 보여주고 있다.

모든 과정은 이전에 설명한 프로토콜과 동일하다. 다만 지불을 수행할 경우 USIM의 지불 데이터를 이용하는 것이 아니기 때문에 가상은행에

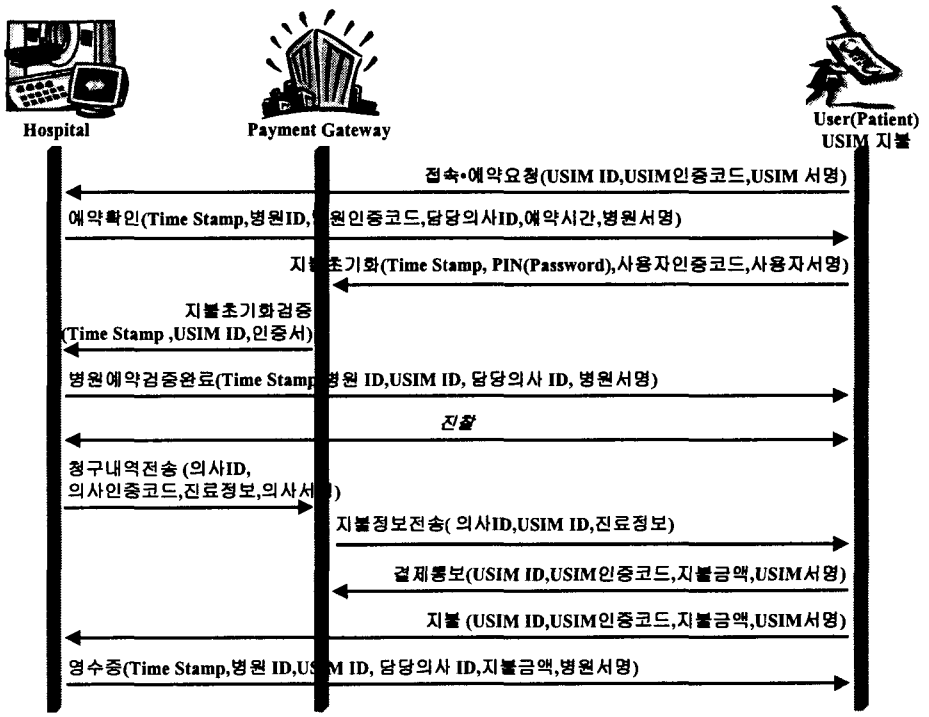

그림 4. USIM을 이용하여 지불을 수행하는 헬스케어 지불 프로토콜

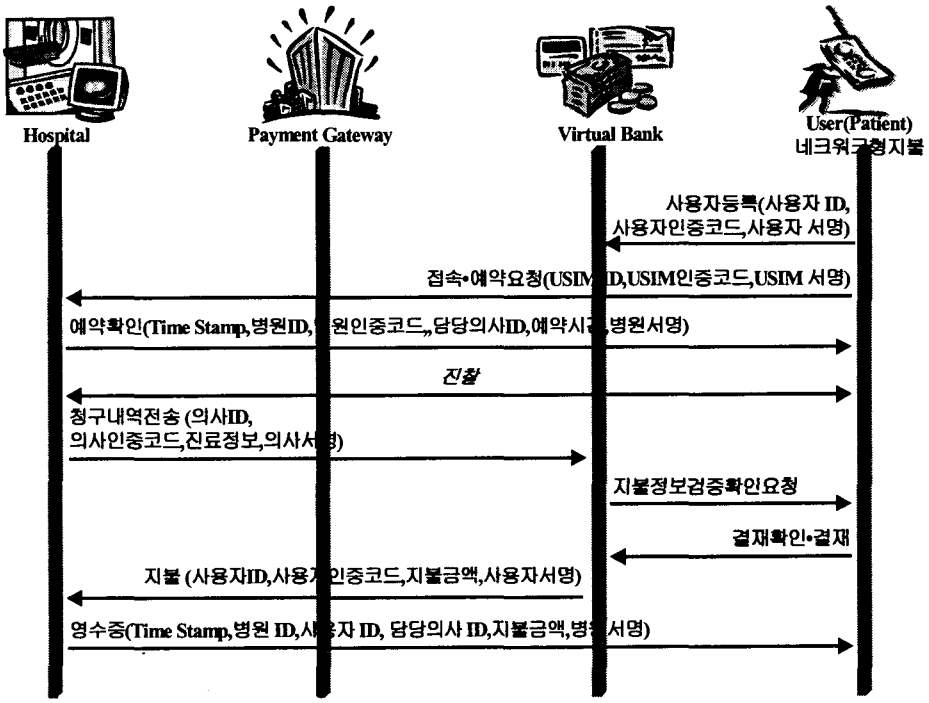

그림 5. 네트워크형 지불을 수행하는 헬스케어 지불 프로토콜

일단 사용자가 등록되어 있어야 하고 지불은 가상 은행을 통해서 수행되는 차이점이 있다.

5. 결 론

본 연구는 모바일 단말기나 PDA와 같은 무선 단말기에 내장되어 있는 USIM을 이용하여 유비쿼터스 시대에 맞는 원격 진료 시스템을 연구하였다. 유비쿼터스 상에서 헬스케어 서비스는 다양한 모델이 제시될 수 있는 광범위한 분야이다. 따라서 본 연구는 병원을 통한 헬스케어 서비스 후의 지불에 초점을 두어 프로토콜을 제시하였다. 프로토콜을 제시하기 전에 헬스케어를 위해 요구되는 보안사항을 분석하였고 다양하게 구성될수 있는 헬스케어 서비스의 전체 구성도를 제안하였으며 특히 지불과 관련된 요소만을 선택하여 지불 프로토콜을 제안하였다. USIM이 제공하는 안전성을 토대로 하여 사용자가 안전하게 헬스정보를 제공받고, 지불할 수 있는 시스템을 제안하였다. 그러나 본 연구의 경우 현실적으로 유비쿼터스 환경은 아직 기초적인 단계로서 완벽한 시스템을 구축하기 위해서는 다양한 연구가 동반 수행되어야 한다. 또한 유비쿼터스 환경에 맞는 다양한 시나리오는 제시되고 있으나 실제로 구현된 사례가 없어 다양한 유비쿼터스의 다양한 응용 서비스 구성에 기초 자료로 활용이 가능하리라 사료된다. 따라서 본 논문에서 제안된 방식의 경우 헬스케어 뿐만 아니라 경제. 사회, 문화 등 각종 분야에 영향을 미칠 수 있는 IT기술이므로 다양한 비즈니스 모델 및 시나리오를 제안하고 시스템을 구축할 수 있도록 연구가 지속 되어야 할 것이다.

참 고 문 헌

[1] Maritin Reichenbach, Hervert Damker, Hannes Federrath and Kai Rannenberg., "Individual Management of Personal Reachability in Mobile Communication", Information Security in Reserch and Business; 13th international conference on Information Security, Chapman &Hall, May 1997. p. 164-174.

[2] Toshitada NAGUMO, "Innovative Business Models in the Era of Ubiquitous Networks", NRI Papers NO.49, June 1, 2002.

[3] Hideaki NAKAMOTO, Nakoto SHIROTA, "System Integration Technology in the Ubiquitous Network Era", NRI Papers NO.64, May 1, 2003.

[4] Anderson, N., Janson, P., Waidner, M., "The State of the art in Electronic Payment System", Advances in Computers, 53, 2000.

[5] Salla Kalaja, "Security in Mobile Health Care Work", Tik-110.501 Seminar on Network Security, 2000.

[6] Dieter Gollmann, "Computer Security", John Wiley&Sons, 1999.

[7] Dimitri Konstantas, Val Jones, "MobiHealth-innovative 2.5/3G mobile services and application for healthcare", NEC Research, 2000.

[8] Ramon Marti, Jaime Delgado, "Security in a Wireless Mobile Health Care System", NEC Research, 2000.

[9] Hendry, M., "Smart Card Security and Application", Artech House, Boston/London, 1997.

[10] Zhiqun Chen, "Java Card Technology for Smart Cards", Addison-Wesley, 2000.

[11] MobiHealth(http://www.mobihealth.org)

[12] Healthmate(http://www.Healthmate-Project.org)

[13] Gemplus(http://www.gemplus.com)

[14] Java Card(http://www.java.sun.com/products/javacard)

[15] Mobile Java(http://www.mobilejava.co.kr)

홍 인 식

- 1981년 한양대학교 전자공학과(학사)
- 1986년 한양대학교 대학원 전자공학과(석사)
- 1988년 한양대학교 대학원 전자공학과(박사)
- 1991년~1995년 순천향대학교 공과대학 전산학과 전임강사
- 1995년~1999년 순천향대학교 공과대학 컴퓨터학부 조교수
- 1999년~순천향대학교 공과대학 정보기술학부 부교수
- 관심분야 : 임베디드 시스템, 스마트 카드, 모바일 통신
- E-mail : ishong@sch.ac.kr

백 장 미

- 2001년 순천향대학교 컴퓨터학부 (학사)
- 2002년 순천향대학교 대학원 전산학과 석사과정
- 관심분야 : M-commerce, 스마트 카드, 모바일 통신