http://dx.doi.org/10.14400/JDC.2015.13.1.275

# 계층적 다중 속성을 이용한 헬스케어 환자의 프라이버시 보호 기법

신승수
동명대학교 정보보호학과

# Privacy Protection Scheme of Healthcare Patients using Hierarchical Multiple Property

**Seung-Soo Shin**
**Dept. of Information Security, Tongmyong University**

**요 약** 최근 헬스케어는 다양한 의료 서비스를 제공받으려는 사용자가 급격하게 증가하고 있으며, 환자의 정보가 제3자에게 쉽게 노출되어 악용될 수 있어 환자에 따라 병원 관계자(의사, 간호사, 약사 등)의 역할이 명확하게 분류될 필요가 있다. 본 논문에서는 헬스케어 환경에서 환자의 정보가 제3자로부터 안전하게 사용하기 위해서 환자의 속성정보를 분류하고, 병원 관계자는 역할에 따라 권한을 분류하여 계층적 다중 속성을 이용한 환자의 프라이버시 보호기법을 제안한다. 제안 기법은 환자의 프라이버시 속성정보(데이터 소비자, 시간, 센서, 목적, 의무, 위임 그리고 상황 등)를 수학적 모델로 표현하고, 제 3자로부터 환자 정보가 불법적으로 악용되는 것을 예방하기 위해서 환자와 병원관계자 사이의 속성정보를 동기화하여 환자의 프라이버시 정보의 유출을 예방한다.

**주제어** : 다중 속성, 접근 제어, 프라이버시, 헬스 케어, 서비스거부공격

**Abstract** The recent health care is growing rapidly want to receive offers users a variety of medical services, can be exploited easily exposed to a third party information on the role of the patient's hospital staff (doctors, nurses, pharmacists, etc.) depending on the patient clearly may have to be classified. In this paper, in order to ensure safe use by third parties in the health care environment, classify the attributes of patient information and patient privacy protection technique using hierarchical multi-property rights proposed to classify information according to the role of patient hospital officials The. Hospital patients and to prevent the proposed method is represented by a mathematical model, the information (the data consumer, time, sensor, an object, duty, and the delegation circumstances, and so on) the privacy attribute of a patient from being exploited illegally patient information from a third party the prevention of the leakage of the privacy information of the patient in synchronization with the attribute information between the parties.

**Key Words :** Multiple Property, Access Control, Privacy, Healthcare, Denial of Service

* 본 논문은 2013년 동명대학교 교내 학술연구비에 의하여 지원되었음
Received 25 November 2014, Revised 26 December 2014
Accepted 20 January 2015
Corresponding Author: Seung-Soo Shin
(Dept. of Information Security, Tongmyong University)
Email: shinss@tu.ac.kr

ISSN: 1738-1916

## 1. 서론

최근 의료 서비스 분야에서는 사물인터넷 개념을 적용한 서비스, 즉, 각종 웨어러블 기기나 스마트 기기와 연동해 신체의 정보를 감지하고 그 데이터를 수집해 환자의 건강상태를 보다 효율적으로 관리할 수 있는 헬스케어 서비스가 각광을 받고 있다[1,2].

과거보다 IT 기술이 급격히 발달하면서 IT 기술이 접목된 헬스케어 서비스 개념이 계속 나타나고 있다[3,4,5]. 2014년 삼성전자는 미국에서 '삼성 디지털 헬스' 서비스를 발표하였다. 삼성 디지털 헬스는 사물인터넷 기술이 헬스케어에 접목된 건강관리 플랫폼으로, IT 기기를 통해 건강상태를 확인하고 분석함으로써 효율적인 건강관리를 할 수 있도록 돕는 서비스이다. 디지털 헬스케어 IT 기기는 생체 센서가 탑재되어 사용자의 생체신호를 감지하는 손목밴드 형태의 하드웨어 '심밴드'와 수집한 데이터를 가지고 사용자의 건강상태를 분석하는 클라우드 기반의 소프트웨어 '사미'로 구성된다. 심밴드가 매일 사용자의 호흡이나 혈압 등을 체크하면 사미가 이를 분석하여 사용자의 건강상태의 변화나 주의점 등을 바로 알려주는 등의 방식으로 동작된다.

기존 의료서비스 기술에 접목하여 언제, 어디서나, 보건의료 서비스를 제공하더라도 헬스케어 서비스는 바이오정보를 포함한 개인정보와 의료정보를 다루기 때문에 해킹으로 인한 정보유출 사고발생시 국가적인 혼란과 사회적인 불신을 야기할 수 있는 문제점이 있다[2]. 헬스케어 서비스는 사용자가 일일이 건강 상태를 체크하지 않아도 사물인터넷이 적용된 IT 기기와 클라우드 기반 소프트웨어를 통해 더 편리하면서 안전하게 건강관리를 할 수 있어야 한다.

환자의 개인건강정보(Personal Health Information)는 환자에게 매우 민감하기 때문에 제 3자에게 쉽게 노출될 경우 개인의 프라이버시 침해가 심각해 질 수 있다. 환자의 개인 건강정보의 프라이버시 노출을 최소화하기 위해서는 환자와 병원 관계자사이에서는 개인 건강정보의 의존도 및 접근제어를 높게 유지하는 방법과 헬스케어 응급상황 기술이 필요하다.

본 논문에서는 헬스케어 서비스를 제공받는 환자가 제 3자에게 환자의 프라이버시 정보를 유출하지 않는 다중 속성기반 환자의 프라이버시 기법을 제안한다. 제안 기법은 환자의 속성정보를 9개로 분류하여 환자 상태에 따라 속성정보를 조합하여 환자의 프라이버시를 보호한다. 또한, 병원 관계자도 권한 속성정보를 추출하여 환자의 프라이버시 정보 접근에 제한을 둔다. 또한 제 3자로부터 환자정보가 불법적으로 악용되는 것을 예방하기 위해서 환자와 병원 관계자 사이의 속성 정보를 동기화함으로써 환자의 개인정보의 유출을 예방할 수 있다.

이 논문의 구성은 다음과 같다. 2장에서는 헬스케어와 m-헬스케어 서비스 개념 및 보안 문제에 대해서 알아본다. 3장에서는 계층적 다중 속성기반의 환자 프라이버시 보호 기법을 제안하고, 4장에서는 제안 기법의 보안 평가를 분석하고 마지막으로 5장에서 결론을 맺는다.

## 2. 관련연구

### 2.1 헬스케어 서비스

헬스케어 서비스는 IT 기술을 보건의료산업에 접목하면서 인체의 건강 관련 정보를 언제, 어디서나, 수집, 처리, 전달, 관리 할 수 있게 함으로써 제공되는 환자의 건강 및 의료서비스를 의미한다[1,2].

헬스케어 서비스의 진행 과정은 4단계로 구성된다. 1단계는 센싱 단계로써 환자의 인체에서 발생하는 물리적 화학적인 현상을 감지하는 단계이다. 이 단계는 인체에서 발생하는 물리적・화학적인 현상의 변화를 감지하여 처리 가능한 전기적 신호로 변환하는 곳이다. 2단계는 모니터링 단계로써 환자의 인체에서 측정된 생체정보를 1차적으로 가공하는 단계이다. 이 단계는 측정된 생체정보를 의미 있는 생체신호 성분만을 선택하기 위한 필터링 처리와 의미 있는 정보로 만들기 위한 분석과정, 그리고 이를 시각화하기 위한 과정으로 구성된다. 3단계는 분석 단계로써 측정된 환자의 데이터를 종합하여 종합적인 건강지표를 작성하는 단계이다. 이 단계는 단순히 현재의 상태를 모니터링 할 뿐만 아니라, 장시간에 걸쳐 측정된 데이터로부터 건강상태, 생활패턴 등을 나타내는 새로운 건강자료를 분석한다. 4단계는 피드백 단계로써 건강상태의 변화를 사용자에게 알리는 단계이다. 이 단계는 장시간에 걸쳐 파악된 건강 기지선이나 생활의 변화를 사용자의 행동변화, 경고등으로 사용자에게 제공하는 과정이다[4,6].

### 2.2 m-헬스케어 서비스

m-헬스케어 서비스는 홈네트워크 상의 장치나 휴대용 장치 등의 정보통신기술이 의료와 접목되어 생체 정보를 실시간으로 모니터링하고 자동으로 병원 및 의사와 연결되어 시간과 공간에 구애 받지 않고 언제 어디서나 건강을 관리하고 증진시키며 질병을 예방하고 관리하는 새로운 형태의 의료 서비스를 의미한다[2,3]. m-헬스 케어는 과거 전통적인 헬스케어의 영역에서 물리적, 시간적으로 제약되어 있던 서비스의 편리성을 높이기 위해 유·무선 온라인 네트워크를 활용하여 전자적 의료정보 및 진료 예약관리 등을 제공하던 e-헬스케어 단계에서 한 단계 더 진화된 서비스이다[6].

의료 서비스 기술이 발달함에 따라 m-헬스케어의 의료정보 보안에 대한 요구가 급증하고 있으며, PKI 또는 데이터 암호화 등을 중심으로 보안 기술들을 제품에 적용하고 있다[7,8]. m-헬스케어 환경에서 데이터 보호 및 프라이버시 보호 문제와 관련된 다양한 보안 취약점과 위협 요소들은 유·무선 네트워크 기반 서비스에서 발생 가능한 보안상 취약점과 유사하다. 그러나 m-헬스케어 서비스는 기존 유·무선 네트워크 기반 서비스와는 다른 보안 요구사항들이 존재한다[7,8,9]. m-헬스케어에 사용되는 새로운 장비들과 네트워크상에서 존재하는 신규 취약점에는 첫째, 서비스를 지원하는 서버를 공격하는 DoS 공격 유형, 둘째, 바이러스/웜 해킹 공격 유형, 셋째, 의료정보 도청/위변조 공격 유형, 넷째, 유·무선 인프라에서 가능한 여러 불법 접근 공격 유형, 다섯째, 오프라인을 통한 방범 시스템 고장 및 인위적인 기기 마비, 방해 전파, 화재와 같은 인재 또는 악의적인 행위를 통한 공격 유형 등이 있다[10,11,12].

## 3. 다중 속성기반 환자의 프라이버시 보호 기법

이 절에서는 헬스케어 환경에서 다양한 의료 서비스를 제공받는 환자의 여러 속성 정보에 따라 환자의 프라이버시를 보호할 수 있는 기법을 제안한다.

### 3.1 개요

헬스케어 환경에서 의료 서비스를 제공받는 사용자의 프라이버시를 보장하기 위한 환자의  속성 정보는 데이터 소비자, 시간, 센서, 목적, 의무, 위임 그리고 상황 등이 있다. 환자의 속성 정보는 의료 서비스를 제공 받는 환자에게 특정 권한을 부여받는 동시에 필요한 정책을 적용받는다. 또한, 제안 모델에서 환자의 속성 정보는 환자의 의료정보의 중요도에 따라 보안정책, 접근 정책을 포함한 특정 역할을 부여받는다. 환자 개인에 대한 개별 정보들에 대한 접근 권한은 정책의 변경 없이도 역할의 변경을 통해 다양한 정책을 할당받는다. 제안 모델은 병원과 관련된 자원의 역할 및 권한에 따라 사용자의 데이터베이스 접근을 제어한다.

최근 환자의 프라이버시 위협이 증가되는 환경에서 병원이나 약국이 환자의 기록을 악용할 경우, 제안 모델에서는 병원이나 약국에게 제한된 권한을 부여하여 환자의 동의에 따라 진찰 및 치료 내역을 이용할 수 있다.

제안 모델에서는 사용자의 권한 확인 및 기록 접근제어 등을 통하여 환자, 병원, 약국의 권한을 분리하여 최소한의 업무만을 수행한다. 그 결과, 제 3자는 쉽게 환자의 민감한 의료정보 및 개인정보에 접근하지 못한다.

### 3.2 용어 정의

<Table 1>은 제안된 프로토콜에서 사용하는 용어에 대한 설명이다.

〈Table 1〉 Notation

| Notation | Definition |
|---|---|
| $SC$ | Service Center |
| $U_i$ | $i^{th}$ patient |
| $\vec{p}$ | Personal Information of Patient |
| $P_i$ | $i^{th}$ Hospital Manager |
| $ID_i$, $ID_j$ | Unique Identifier of $U_i$ and $P_i$ |
| $ak_i$ | Access key of Patient |
| $sk_i$ | Secret key of Patient |

### 3.3 속성 기반 환자 프라이버시 보호 처리

헬스케어 환경에서 환자가 진료 과정에서 환자의 프라이버시를 보호받기 위해서 환자의 프라이버시 속성정보(데이터 소비자, 시간, 센서, 목적, 의무, 위임 그리고 상황 등) 부여 과정이 필요하다. 이 절에서는 환자의 프

라이버시를 협상하기 위한 환자의 프라이버시 속성정보를 수학적 모델로 표현한다.

#### 3.3.1 환자의 프라이버시 규칙

이 과정에서는 환자의 프라이버시를 보장하기 위한 속성 정보들의 규칙을 정의한다. 환자의 프라이버시 규칙들은 조건(Condition)과 동작(Action)으로 구분되며, 환자의 프라이버시에 대한 접근 제어를 수행하기 위해 <Table 2>과 같은 정보를 포함한다. 데이터 제공자들은 자신들의 프라이버시 규칙을 <Table 2>를 참조하여 정의한 후 데이터베이스에 저장한다.

〈Table 2〉 Status and Action Rule of patient

| Option | | Property |
|---|---|---|
| Status | Data sharer | User name, group name etc. |
| | Purpose | Use purpose |
| | Obligation | Obligations |
| | Mandate | Delegator |
| | Location | Predefined tables, local coordinates |
| | Time | Time range, repetition time |
| | Sensor | Sensor channel name |
| | Status | situation which can be used in sensor |
| Action | | Action, activity |

#### 3.3.2 환자의 프라이버시 속성 부여

이 과정은 환자가 의료 서비스를 제공받는 과정에서 환자의 속성을 부여받을 수 있는 정보들을 상관관계 행렬로 표현하는 과정이다.

환자의 속성 정보는 의료 서비스 과정에서 부여받은 데이터 소비자, 시간, 센서, 목적, 의무, 위임 그리고 상황 등 9가지의 정보이며, 이 정보들의 상관관계 행렬은 식 (1)처럼 나타낸다. 식 (1)에서 협상을 위한 정보는 9 가지 정보라고 가정한다. 식 (1)에서 $k$는 환자의 속성 정보의 개수를 의미하며, $k$의 범위는 1 부터 9 까지를 의미한다.

$$Co_{attr_i} = \begin{Bmatrix} 0 & \lambda_{12} \cdots \lambda_{1k} \\ \lambda_{21} & 0 \cdots \lambda_{2k} \\ \vdots & \vdots \ddots \vdots \\ \lambda_{k1} & \lambda_{k2} \cdots 0 \end{Bmatrix} \quad (1)$$

여기서, $\lambda_{mn}$는 환자의 속성 정보 $attr_i$와 $attr_j$ 사이의 상관정보를 의미하고, $\lambda_{mn}$ 와 $\lambda_{nm}$는 $m$이 0 이상이고 $n$이 1 미만($0 \le m, n \le 1$)인 조건에서 동일하다. 만일 $\lambda_{mn}$이 0 이면 속성 정보 $attr_i$와 $attr_j$ 사이의 상관관계는 없다.

#### 3.3.3 환자의 속성 정보 처리 과정

이 과정은 헬스케어 환경에서 갑작스런 의료 서비스를 환자가 요청할 경우 환자의 속성 정보를 처리하는 과정이다.

- 단계 1 : 헬스케어 환경에서 환자 $U_i$는 의료서비스를 제공받기 전 환자 $U_i$의 속성 정보를 이용하여 식 (1)처럼 환자 $U_i$의 프라이버시 정보 $\vec{p}$을 서비스센터 $SC$가 생성한다.

$$\vec{p} = (Co_{attr_1}, Co_{attr_2}, \cdots, Co_{attr_n}) \quad (2)$$

여기서, $n$은 환자의 속성 정보의 수를 의미한다.

- 단계 2 : 환자의 프라이버시 정보 $\vec{p}$가 생성되면 환자 $U_i$의 개인정보 $\vec{p}$에 접근하기 위한 랜덤 키를 식 (3)처럼 2 개 생성한다.

$$(t_1, t_2) \in \mathbb{Z}_q^* \quad (3)$$

- 단계 3 : 병원 관계자 $P_i$는 식 (3)에서 생성한 2개의 랜덤 키를 이용하여 환자 $U_i$의 접근제어 키 $ak_i$와 비밀키 $sk_i$을 식 (4)~(5)처럼 생성한다.

$$ak_i = (q^{x+at_1}, q^{t_1}, q^{t_2}) \quad (4)$$

$$sk_i = H(UI_i \parallel \vec{p} \parallel ak_i) \quad (5)$$

- 단계 4 : 병원 관계자 $P_i$는 환자 $U_i$의 속성 정보를 환자에게 전달하여 환자의 상태 $State$을 갱신한다. 환자의 상태 $State$는 0 과 1 의 값에 따라 정보의 갱신 유·무를 판별한다.

• 단계 5 병원 관계자 $P_i$는 환자 $U_i$의 프라이버시 정보 $\vec{p}$을 식 (6)처럼 수집한다.

$$Gathering\ \vec{p} = (a_1, a_2, \cdots, a_n) \quad (6)$$

식 (6)처럼 환자 $U_i$의 프라이버시 정보 $\vec{p}$을 수집하는 병원 관계자 $P_i$는 환자에게 응급상황이 발생할 경우 병원 관계자 $P_i$는 데이터베이스에 저장되어 있는 환자 $U_i$의 상태정보 $State$을 점검한다. 만일 상태정보 $State$가 정상이면 환자의 개인정보를 모니터링하고 그렇지 않으면 종료한다.

#### 3.3.4 병원 관계자의 접근 제어 과정

이 과정은 병원 관계자 $P_i$가 환자 $U_i$의 프라이버시 정보 $\vec{p}$에 접근하는 것을 제어하는 단계이다.

• 단계 1 : 병원 관계자 $P_i$는 권한 속성 정보 $M_l$을 식 (7)처럼 추출한다.

$$M_l = \{M_l \mid M_l \in M, 1 \le l \le L\} \quad (7)$$

여기서 $L$은 분산된 병원 관계자 정보의 총 개수를 의미한다. 단, $M$은 $M_1 \cup M_2 \cup \cdots \cup M_L$이고 $\varnothing = M_1 \cap M_2 \cap \cdots \cap M_L$이라고 가정한다.

• 단계 2 : 병원 관계자 $P_i$는 소수 $q(q \ge n+1)$를 선택한 후 $\mathbb{Z}_q$에서 임의의 랜덤 수 $a_i(1 \le i < t)$를 선택하여 이진수 $k$로 변환한다. 변환된 이진수 $k$을 상수항으로 하는 임의의 다항식 $a_{(n-1)(k-1)} + a_{(n-1)k}$이 생성되면 식 (8)처럼 다항식을 $a_{nk}$로 변환한다. 여기서, 다항식 $a_{(n-1)(k-1)} + a_{(n-1)k}$는 병원 관계자의 권한 정보를 트리구조의 계층적 형태로 정보를 생성된다.

$$a_{nk} = a_{(n-1)(k-1)} + a_{(n-1)k}\ (n,k > 1) \quad (8)$$

• 단계 3 : 병원 관계자 $P_i$의 권한 정보 $a_{nk}$가 $n$번째 줄의 $k$번째 값이라고 하면, $n$번째 열의 $k$번째 값은 $\binom{n-1}{k-1}$과 같은 병원 관계자의 권한 정보값을 구한다. 관리자는 병원 관계자에게 추출된 권한정보에 따른 환자의 생체정보를 전달한다.

$$a_{nk} = a_{(n-1)(k-1)} + a_{(n-1)k}\ (n,k > 1) \quad (9)$$

이때,

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \quad (10)$$

같은 성질을 이용하여 식 (9)처럼 병원 관계자의 속성 정보 값을 추출한다.

$$a_{nk} = \binom{n-1}{k-1} \quad (11)$$

## 4. 보안 평가

제안 모델에서는 환자 $U_i$의 프라이버시를 보호하기 위해서 환자 $U_i$의 다중 프라이버시 정보 $\vec{p}$와 병원 관계자 $P_i$의 권한 속성정보 $M_l$을 이용한다. 환자 $U_i$의 다중 프라이버시 정보 $\vec{p}$와 병원 관계자 $P_i$의 권한 속성정보 $M_l$는 환자 $U_i$의 프라이버시에 제 3자가 접근하는 것을 제어한다. 특히, 병원 관계자 $P_i$의 권한정보를 임의의 다항식으로 만들어 병원 관리자 $P_i$의 접근 권한을 만들기 때문에 기존 프라이버시 보호 기법보다 단순하면서도 효율적으로 환자 $U_i$의 프라이버시를 보장할 수 있다. 또한, 병원 관리자 $P_i$의 권한정보 $a_{nk}$는 제 3자의 접근을 엄격하게 제약하기 때문에 안전하다.

제안 모델에서는 환자 $U_i$의 생체정보에 접근하는 병원 관리자 $P_i$의 권한정보를 추출하기 위해서 타임스탬프 동안 병원 관리자 $P_i$의 권한정보를 유지하기 때문에 병원 관계자 $P_i$의 권한정보에 대한 최신성을 유지한다. 또한, 병원 관리자 $P_i$의 권한정보에 대한 접근제어를 통해 환자 $U_i$의 생체정보의 최신성을 보장하여 서비스 거부 공격을 방지한다.

병원 관리자 $P_i$는 환자의 생체정보를 요청하는 병원 관리자 $P_i$의 활동을 엄격하게 제약하기 위해서 병원 관리자 $P_i$의 권한등급에 따라 환자의 생체정보의 접근을 제약하고 있다. 제안 모델에서는 신분 및 인증을 병원 관리자 $P_i$의 권한 속성정보를 바탕으로 처리하기 때문에 병원 관리자의 속성정보 $M_l = \{M_l \mid M_l \in M, 1 \leq l \leq L\}$로 환자 $U_i$의 생체정보 접근을 제어한다.

제안 모델에서는 2개 이상의 병원에서 환자의 생체정보를 요청할 경우 병원 관계자의 권한속성에 대한 정보를 모두 보유하여야 한다. 타 병원에서는 일정 시간 간격 사이로 권한 속성정보가 변경될 수 있다. 제안 모델에서는 병원 $H_i$에서 병원 $H_j$로 환자의 생체정보 요청이 있을 경우 공개키로 암호화하고 복호화하는 과정이 홉-대-홉 방식으로 진행되기 때문에 Sybil 공격에 안전하다.

제 3자가 환자 $U_i$의 개인건강정보 $PHI_i$을 추출하려고 시도하더라도 프라이버시 정보 $\vec{p}$ 부족과 접근제어 키 $ak_i = (q^{x+at_1}, q^{t_1}, q^{t_2})$를 생성하기 위한 랜덤 수 $t_1$, $t_2$을 제 3자가 모르기 때문에 비밀키 $sk_i$ 및 공유키 $K_i$을 액세스 할 수 없다. 제안 기법에서 범위 내에 위조된 환자 $U_i$의 개인건강정보 $PHI_i$을 삽입하려고 하는 침입 노드를 예방하기 위한 방법은 간단하며 지연 없이 수행될 수 있다. 병원 관계자 $P_i$는 모든 전송된 데이터를 조사하여 접근제어 키 $ak_i = (q^{x+at_1}, q^{t_1}, q^{t_2})$가 누설될 경우 위조 전송을 탐지한다.

## 5. 결론

본 논문에서는 헬스케어 환경에서 의료서비스를 제공받는 환자의 프라이버시 정보를 다중 속성정보를 이용하여 환자의 프라이버시를 보호할 수 있는 기법을 제안하였다. 제안 기법은 환자의 프라이버시 보호를 위해 환자에게는 9개의 속성정보를 부여하고 병원 관계자에게는 환자에게 접근할 수 있는 권한 속성정보를 부여하였다. 또한 제 3자로부터 환자정보가 불법적으로 악용되는 것을 예방하기 위해서 환자 $U_i$와 병원 관계자 $P_i$ 사이에서 생성된 접근제어 키 $ak_i = (q^{x+at_1}, q^{t_1}, q^{t_2})$, 비밀키 $sk_i (= H(UI_i \| \vec{p} \| ak_i))$ 등을 동기화하여 개인건강정보의 유출을 예방하였다. 향후 연구에서는 병원과 환자사이에서 안전한 환자의 개인건강정보를 확장하여 다수의 병원에서 환자의 개인건강정보를 통합운영 관리할 수 있도록 프레임워크를 개발할 예정이다.

## ACKNOWLEDGMENTS

This research was supported by the Tongmyong University of Research Grants 2013(2013A012).

## REFERENCES

[1] T. M. Song, S. H, Jang, "u-Healthcare : Issue and Research Trends", Korea Institute for Health and Social Affairs, pp. 119-129, 2011.

[2] J. Zhou, Z. Cao, X. L. Dong, X. D. Lin, "Securing m-healthcare social networks: challenges, countermeasures and future directions", IEEE Wireless Communications, Vol. 20, No. 4, pp. 12-21, 2013.

[3] R. X. Lu, X. D. Lin, X. M. Shen, "SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency", IEEE Transaction on Parallel and Distributed Systems, Vol. 24, No. 3, pp. 614-624, 2013.

[4] F. Miao, L. Jiang, Y. Li, Y. T. Zhang, "Biometrics based novel key distribution solution for body sensor networks", 2009. Annual International Conference of the IEEE Engineering in Medicine and Biology Society(2009 EMBC), pp. 2458-2461, 2009.

[5] F. Miao, L. Jiang, Y. Li, Y. T. Zhang, "A Novel Biometrics Based Security Solution for Body Sensor Networks", 2nd International conference on biomedical Engineering and Informatics 2009(BMEI '09), pp. 1-5, 2009.

[6] G. Sudha, R. Ganesan, "Secure transmission medical data for pervasive healthcare system using android", 2013 International Conference on Communications

and Signal Processing(ICCSP), pp. 433-436, 2013
[7] U. Harish, R. Ganesan, "Design and development of secured m-healthcare system", 2012 International conference on Advances in Engineering, Science and Management(ICAESM), pp. 470-473, 2012.
[8] M. Y. Hwang, C. H. Jin, U. Yun, K. D. Kim and K. H. Ryu, "Building of prediction model of wind power generation using power ramp rate", Journal of the Korea Society of Computer and Information, Vol. 17, pp. 211-218, 2012.
[9] Z. Omary, f. Mtenzi, B. Wu, C. O'Driscoll, "Accessing sensitive patient information in ubiquitous healthcare systems", 2010 International conference for internet Technology and Secured Transactions (ICITST), pp. 1-3, Nov. 2010.
[10] D. W. Bang, J. S. Jeong, J. H. Lee, "An implementation of privacy security for PHR framework supporting u-healthcare service", 2010 6th International conference on Networked Computing(INC), pp. 1-4, May. 2010.
[11] K. J. Kim, S. P. Hong, "Privacy Information Protection Model in e-Healthcare Environment", Korean Society for Internet Information, Vol. 10, No. 2, pp. 29-40, Apr. 2009.
[12] D. G. Kim, I. G. Song, "Need and Development of u-Healthcare Service", Korean Society for Internet Information, Vol. 1, No. 3, pp. 9-17, Sep. 2009.

**신 승 수(Shin, Seung Soo)**

・2001년 2월 : 충북대학교 수학과 (이학박사)
・2004년 2월 : 충북대학교 컴퓨터공학과(공학박사)
・2005년 ~ 현재 : 동명대학교 정보보호학과 부교수
・관심분야 : 네트워크보안, USN, 스마트카드, 헬스케어보안.
・E-Mail : shinss@tu.ac.kr