https://doi.org/10.14400/JDC.2017.15.3.187

IoT 기반의 모바일 헬스케어 서비스를 위한 데이터 저장 및 보호 모델

정윤수
목원대학교 정보통신융합공학부

Data Storage and Security Model for Mobile Healthcare Service based on IoT

Yoon-Su Jeong
Dept. of Information Communication & Engineeringe, Mokwon University

요 약 사물인터넷 기반의 헬스케어 서비스는 다양한 사물인터넷 디바이스를 통해서 사용자의 생체신호 측정, 질병 진단 및 예방을 포함한 건강관리 및 의료 서비스를 제공하고 있다. 그러나, 사물인터넷 기반의 헬스케어 서비스는 여러 가지 요소 기술들이 통합되어 서비스를 제공하기 때문에 각 요소 기술 자체의 보안 취약성과 연동 시 새로운 보안 취약성이 발생할 수 있는 문제점이 존재한다. 본 논문에서는 모바일 환경에서 IoT 기반의 웨어러블 장비를 이용한 사용자의 헬스케어 정보를 서버에 전달할 때 제 3자로부터 사용자의 헬스케어 정보를 안전하게 처리할 수 있는 사용자 프라이버시 보호 모델을 제안한다. 제안 모델은 사용자의 헬스케어 정보를 안전하게 처리, 보관, 저장할 수 있도록 헬스케어 센서 정보 별로 속성 값을 부여하여 사용자의 프라이버시를 계층적으로 통합 관리한다. 성능평가 결과, 제안모델은 기존모델보다 IoT 장치의 처리율은 평균 10.5% 향상되었고, 서버의 오버헤드는 기존 모델에 비해 평균 9.9% 낮은 결과를 얻었다.

주제어 : 헬스케어, 사물인터넷, 의료 서비스, 모바일, 프라이버시

Abstract Objects Internet-based healthcare services provide healthcare and healthcare services, including measurement of user's vital signs, diagnosis and prevention of diseases, through a variety of object internet devices. However, there is a problem that new security vulnerability can occur when inter-working with the security weakness of each element technology because the internet service based on the object Internet provides a service by integrating various element technologies. In this paper, we propose a user privacy protection model that can securely process user's healthcare information from a third party when delivering healthcare information of users using wearable equipment based on IoT in a mobile environment to a server. The proposed model provides attribute values for each healthcare sensor information so that the user can safely handle, store, and store the healthcare information, thereby managing the privacy of the user in a hierarchical manner. As a result of the performance evaluation, the throughput of IoT device is improved by 10.5% on average and the server overhead is 9.9% lower than that of the existing model.

Key Words : Healthcare, Internet of Things, Hospital Service, Mobile, Privacy

* 본 연구는 산업통상자원부 지역혁신센터사업인 민군겸용보안공학연구센터 지원으로수행되었음.
Received 21 December 2016, Revised 28 February 2017
Accepted 20 March 2017, Published 28 March 2017
Corresponding Author: Yoon-Su Jeong(Mokwon University)
Email: bukmunro@mokwon.ac.kr

ISSN: 1738-1916

1. 서론

최근 사물인터넷(IoT, Internet of Things) 기술의 발전으로 인하여 언제 어디서나 사물들 간 연결이 가능한 시대가 의료・전자 분야를 중심으로 추진되고 있다[1,2]. 사물 인터넷은 환경, 에너지, 재난・재해 등 국가적 현안을 해결할 수 있는 수단인 동시에 비용 절감, 운영 효율화, 신규 서비스 창출 등 기업 경쟁력 강화를 위한 수단으로 활용되고 있다. 특히, 사물인터넷이 적용 가능한 헬스케어 분야는 새로운 시장 창출이 가능하며, 의료비 절감 및 서비스 향상을 실현할 수 있다[3]. 헬스케어 서비스는 향후 질병의 치료보다는 예방과 관리를 중요시하며, 진단, 수술 및 치료에도 확대 적용 가능한 서비스이다[4].

헬스케어 분야는 사람들 사이에서 'Next Big Thing'으로 불리며 많은 기대를 받고 있다[5,6,7]. IT 기술 중 사물인터넷(IoT, Internet of Things)기술과 융합하여 서비스를 제공하기 때문에 의료 분야는 다음과 같이 다른 분야들과 차별성을 가진다[8,9]. 첫째, 개인 유전 정보 분석이다. 유전 정보 분석에 들어가는 시간과 비용이 급격하게 줄어들면서 개인들이 자신의 유전 정보를 분석, 보유, 활용할 수 있다. 둘째, 확대되는 암 환자들의 맞춤 치료가 가능하다. 암은 유전적인 요인 때문에 발병하지만 사람마다 그 유전적 원인이 다르기 때문에 암을 일으키는 유전적인 원인을 분석하고, 그에 맞는 표적 항암적 치료를 받을 수 있다. 셋째, 장소, 시간 상관없이 헬스케어 서비스를 제공받는다. 헬스케어 서비스는 IoT 장치를 몸에 부착하여 사용자의 생체정보를 유・무선 네트워크를 통해 서버에 전달하여 의료진이 사용자의 건강상태를 점검받을 수 있다. IoT 기술을 이용하여 헬스케어에 사용되는 장치들은 Fig. 1과 같다. Fig. 1과 같은 장비들은 인터넷 프로토콜(CoAP/DTLS 또는 HTTP/TLS 등)이 탑재되어 장치를 구성하고 있는 다양한 센서들과 함께 동작하여 사용자에게 서비스를 제공한다[10,11].

본 논문에서는 모바일 환경에서 IoT 기반의 웨어러블 장비를 이용한 사용자의 헬스케어 정보를 서버에 전달할 때 제 3자로부터 사용자의 헬스케어 정보를 안전하게 처리할 수 있는 사용자 프라이버시 보호 모델을 제안한다. 제안 모델은 사용자의 헬스케어 정보를 안전하게 처리, 보관, 저장할 수 있도록 헬스케어 센서 정보 별로 속성값을 부여하여 사용자의 프라이버시를 계층적으로 통합관리한다. 제안 모델은 센서가 탑재된 장비(e.g. 팔찌, 목거리 등)와 휴대폰을 이용하여 사용자의 헬스케어 정보를 확인하고 처리할 수 있도록 사용자 프라이버시 보호 절차를 간소화하였다.

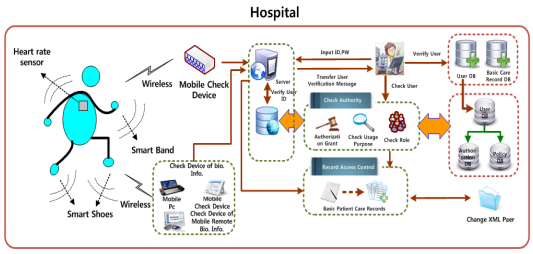
이 논문의 구성은 다음과 같다. 2장에서는 IoT 헬스케어와 기존 연구에 대해서 알아본다. 3장에서는 IoT 기반의 모바일 헬스케어 서비스를 위한 사용자 프라이버시 보호 모델을 제안하고, 4장에서는 기존 기법과 제안 기법을 비교 평가하고, 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 IoT 헬스케어

전 세계적으로 고령화 추세와 웰빙 추구 경향이 심화되면서 개인 건강관리 및 질병예방에 대한 관심이 증가하고 있다[1]. IoT 헬스케어 서비스는 선진국을 중심으로 각광을 받고 있는 분야로써, IoT 융합 관련 핵심 서비스이다. 특히, IoT 헬스케어 서비스는 사물인터넷 기술이 발전함에 따라 IoT 플랫폼 및 웨어러블 디바이스를 활용한 개인 맞춤형 서비스가 각광을 받고 있다. IoT 헬스케어 서비스는 관련 서비스 산업의 성장과 밀접하게 연관되어 있기 때문에 다양한 서비스 산업과 동반성장하고 있다[12,13].

[Fig. 1]은 IoT 기반의 헬스케어 서비스를 보여주고 있다[2]. [Fig. 1]처럼 IoT 기반의 헬스케어 서비스는 무선 환경을 통해 환자에게 부착된 센서를 통해 송신되는 정보를 의료 기관에서 분석 및 처방을 지원한다.



[Fig. 1] Overall Process of Proposed Model

<Table 1>은 영역별 헬스케어 산업 규모 전망을 예방, 진단, 치료, 사후관리 등 4가지 항목으로 분류하고 있다[8]. <Table 1> 헬스케어 서비스는 예방, 진단, 관리와

관련된 산업 비중이 2010년 32%에서 2020년에는 43%까지 확대될 전망이다.

〈Table 1〉 Prospect of Health Care Industry by Division

Note: (), specific gravity (%)

Division (year)	Prevention	Diagnosis	cure	Vigilance	Sum
2010	2,140(6).	5,700(16)	24,240(68)	3,560(10)	35,640(100)
2015	3,980(8)	9,190(19)	31,420(63)	5,100(10)	49,690(100)
2020	6,860(10)	14,400(21)	39,110(57)	8,230(12)	68,600(100)
Average annual growth rate (2010~2020)	12.4	9.7	4.9	8.7	6.8

Source: Samsung Economic Research Institute(2012. 8)

2.2 기존 연구

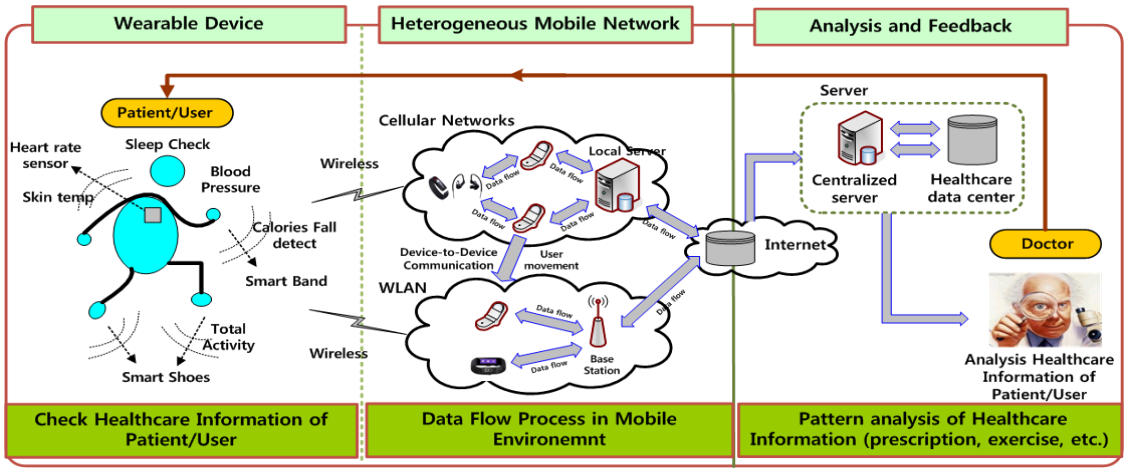
IoT 기반 모바일 헬스케어 서비스를 제공하기 위한 연구가 최근 증가하고 있는 추세이다. Z. A. Khattak et. al는 헬스케어 서비스를 제공하는 사용자의 ID 대신 서버에서 통합 관리하기 위한 연합 ID 관리 모델을 위한 플랫폼을 제안하였다[14]. H. Gao et. al은 헬스케어 서비스가 신뢰할 수 있도록 연합 ID를 이용하여 동적 신뢰 관계를 정책적으로 표현할 수 있는 신뢰 관계 모델을 제안하였다[15]. Y. Zhou et. al은 대리 서명 기법을 위임 검증에 사용되는 대리 서명키를 생성하는 기법을 제안하였다[16]. M. Mambo et. al은 Y. Zhou et. al와 다르게 이산대수문제에 기반한 대리서명기법을 제안하였다. 그러나, 이 기법은 이중 서명 알고리즘을 사용해야 하고 강한 위조 불가능성이 안전하지 않은 문제점이 있다[17]. R. Lu et. al은 위임장과 서명을 전달할 때 소인수 분해 문제의 어려움에 기반하여 대리서명을 생성하는 기법을 제안하고 있다[18]. 그러나, 대리서명자는 인증서의 유효성을 확인해야 하는 문제점이 존재한다.

3. 사용자 프라이버시 예방을 위한 IoT 기반 헬스케어 서비스 모델

현재 IoT 기반 헬스케어를 위해 개발되고 있거나 사용되고 있는 웨어러블 장비들은 모두 서로 다른 플랫폼을 사용하고 있어 사용자 프라이버시에 대한 보안 위협이 증가하고 있다. 이 절에서는 모바일 환경에서 IoT 기반의 웨어러블 장비를 이용하여 헬스케어 서버에 전달되는 사용자의 정보를 제 3자로부터 안전하게 처리할 수 있는 서비스 모델을 제안한다. 제안 모델은 사용자의 진료 환경 개선 및 행정 처리 최소화를 목표로 한다. 제안 모델은 사용자의 헬스케어 정보를 안전하게 처리, 보관, 저장할 수 있도록 사용자의 헬스케어 정보에 속성값을 부여하여 사용자의 프라이버시를 보호한다.

3.1 개요

병원에서 사용하고 있는 IoT 디바이스는 스마트 안경, 스마트 시계, 스마트 슈즈 등과 같은 신체에 손쉽게 착용



[Fig. 2] Overall Process of Proposed Model

할 수 있는 제품이 대부분이다. 현재까지 출시된 제품은 <Table 2>와 같이 기본적으로 항시성, 편의성, 착용감, 안정성 그리고 사회성 과 같은 기능이 제공되고 있다.

〈Table 2〉 Function of Wearable Device

function	Contents
Constant castle	There exists a channel (Internet, Bluetooth, etc.) that can communicate with real time computer
convenience	Provide sense of identity and integration that users can use naturally and conveniently
Fit	When wearing or attaching the user's body, provides lightness and naturalness
stability	Minimize fatigue and skin troubles caused by wearing or attaching for a long time, ensuring safety against power and electromagnetic waves
Sociability	Protection of privacy exposure by recording / recording and hacking

그러나, IoT 기반 헬스케어 장비는 장치간 동기화가 원활하게 이루어지지 않아서 장치를 연동할 경우 오류가 발생할 수 있는 문제점이 존재한다. 제안 모델에서는 IoT 기반의 모바일 헬스케어 서비스를 사용자에게 제공할 경우 IoT 장비가 가지고 있는 속성정보를 활용하여 IoT 장치간 동기화를 손쉽게 유도할 수 있게 함으로써 사용자의 프라이버시를 제공하는 것을 목적으로 한다. 특히, 사용자의 프라이버시를 제3자가 중간에서 가로채어 사용자의 진료 정보를 악용하는 것을 예방하기 위해서 IoT 장치의 접근제어를 지리적 정보와 상태 정보를 행렬의 이진값으로 구성하여 계층화 할 수 있도록 서비스를 제공한다.

[Fig. 2]은 IoT 기반의 웨어러블 장치를 부착한 사용자가 무선 환경을 통해 의료 서버에 사용자의 헬스케어 정보를 전달하여 의료 서비스를 제공받는 구조를 보여주고 있다. [Fig. 2]는 웨어러블 장치, 이질적인 모바일 네트워크, 분석 및 피드백 등 3가지로 구분하여 동작한다. 1단계에서는 사용자가 신체에 부착한 장치(목거리, 스마트 밴드, 스마트슈즈 등)를 통해 심장 박동수, 활동량, 신체 온도, 열 감지 등을 측정한다. 2단계에서는 스마트폰이나 헬스케어 장치를 이용하여 모바일 네트워크 환경을 통해 사용자의 헬스케어 정보를 전달한다. 3단계에서는 무선 환경을 통해 전달된 사용자의 헬스케어 정보를 의료기관의 서버에 저장하여 의료진이 사용자의 헬스케어 정보를 분석하여 사용자의 진료 및 처방을 도울 수 있도록 한다. 또한, [Fig. 2]처럼 제안 모델은 IoT 장비를 통해 사용자의 헬스케어 정보를 서로 다른 네트워크를 통해 전달하여 통합 관리할 수 있다. 제안 모델에서는 IoT 장비를 효율적으로 이용하기 위해서 IoT 장비를 통해 측정된 센싱 데이터를 의료진이 처리하도록 사용자 프라이버시 정보를 계층적으로 분류하여 각 계층별 권한에 맞는 의료 서비스를 제공한다.

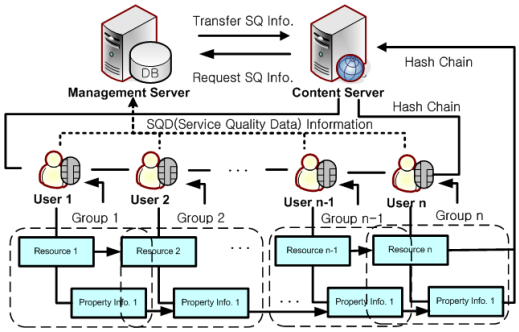
3.2 헬스케어 정보를 이용한 속성 정보의 계층화 과정

제안 모델에서는 IoT기반의 헬스케어 장비를 통해 병원 서버에 사용자의 헬스케어 정보를 저장하여 관리할 수 있도록 사용자의 헬스케어 정보 및 의료진의 신원 정보를 Table 3과 같이 분류한 후 조건과 동작에 따라 속성정보를 부여하여 사용자의 치료 방법 및 기간을 정하여 사용자 스스로 질병 관리할 수 있도록 서비스를 계층화하여 제공한다. 특히, 제안 모델은 Table 3과 같은 속성정보를 이용하여 제3자로부터 사용자의 헬스케어 정보를 불법적으로 악용하지 못하도록 한다[19].

〈Table 3〉 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

또한, 사용자의 헬스케어 정보에 대한 의료진 및 제3자의 접근제어는 [Fig. 3]과 같이 분산 처리할 수 있도록 그룹화하여 처리한다. [Fig. 3]에서 제안 모델은 사용자의 헬스케어 정보에 대한 의료진 및 제3자의 접근제어에 장애가 발생할 경우를 대비하여 보조 서버가 이중 해쉬 처리를 담당하고 있다[13]. 제안 모델의 보조 서버에서 이중 해쉬를 처리하는 이유는 속성 정보를 가진 의료진과 제3자가 사용자의 헬스케어 정보를 권한에 따라 쉽게 접근하기 위해서이다.



[Fig. 3] System Process of Proposed Scheme

제안모델에서 의료진 및 제3자가 악의적으로 사용자의 헬스케어 정보에 접근하려고 할 경우, 제안 모델은 헬스케어 정보의 종류, 기능, 특성에 따라 의료진를 해쉬 체인으로 그룹화하여 의료 서비스를 지원한다. 또한, 의료진의 속성 정보를 제3자에게 노출되었을 때 제안 모델에서는 의료진 및 사용자의 헬스케어 정보 모두에 속성 정보 권한을 부여하여 해쉬 체인으로 그룹화하여 연결한다. 서버는 해쉬 체인으로 그룹화한 연결 정보를 활용하여 의료 서비스를 분산 처리하도록 한다.

3.3 IoT 기반 헬스케어 서비스 과정

제안 모델의 서비스 과정은 IoT 기반의 헬스케어 장비를 통해 서버 데이터베이스에 사용자의 헬스케어 정보를 저장한 후 의료진이 사용자의 헬스케어 정보를 분석하여 피드백하는 과정을 5단계로 구성하여 의료서비스를 제공한다.

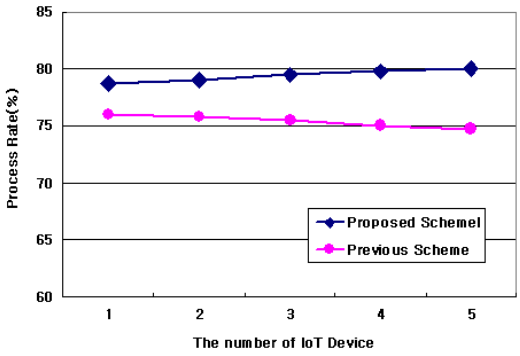
- 단계 1 : IoT 기반 웨어러블 장치를 부착한 사용자는 생체 정보 $\vec{I}(= i_1, i_2, ..., i_n)$를 IoT 기반 웨어러블 장치 수에 따라 각각 생성한다. 여기서 i_i는 웨어러블 장치 수에 따라 수신된 사용자의 생체 정보들을 의미한다.
- 단계 2 : IoT 기반 웨어러블 장치를 통해 생성된 사용자의 생체정보는 스마트폰이나 헬스케어 장치를 이용하여 모바일 네트워크 환경을 통해 사용자의 생체 정보를 전달한다.
- 단계 3: 무선환경을 통해 전달된 사용자의 헬스케어 정보를 의료기관의 서버에 저장한다. 서버에 저장된 사용자의 생체정보는 속성 정보에 따라 사용자의 신체상태 변화에 따라 분류한다.
- 단계 4: 서버에 저장된 사용자의 생체정보를 의료진의 권한에 따라 사용자의 생체 정보를 분석한다. 사용자의 생체 정보가 분석되면 사용자에 맞는 맞춤형 의료 서비스를 제공한다. 특히, 사용자의 질병에 따라 개인 맞춤형 헬스케어 서비스를 제공한다.
- 단계 5: 의료진이 환자의 생체 정보를 분석한 결과를 사용자의 전달한다. 이 때, 권한 등급이 높은 의료진은 사용자와 1:1 면담을 통해 사용자의 건강관리 서비스를 실시간으로 제공할 수 있다.

4. 성능 평가

이 절에서는 IoT 장치의 처리율과 서버의 오버헤드 등을 평가한다. 이 때, 사용자와 서버간 통신은 안전하다고 가정한다.

4.1 IoT 장치의 처리율

[Fig. 4]은 모바일 헬스케어 서비스를 제공받는 사용자의 IoT 장치 수 증가에 따른 IoT 장치에 대한 처리율을 나타내고 있다.



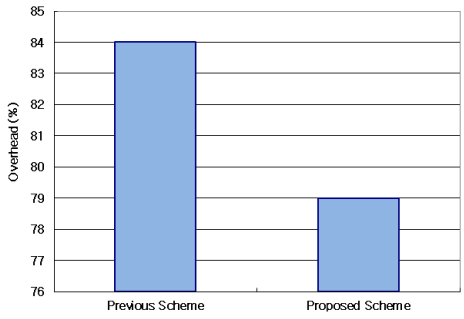
[Fig. 4] Process Rate of IoT Device

[Fig. 4]의 결과, IoT 장치 수가 증가할수록 제안 기법은 비례적으로 IoT 장치의 처리율이 증가하였지만 기존 기법은 IoT 장치 수가 증가할수록 비례적으로 IoT 장치의 처리율이 감소한 결과를 얻었다. IoT 장치의 처리율은 제안 기법이 기존 기법에 비해 IoT 처리율이 10.5% 향상되었다. 이 같은 결과는 의료진 및 제3자의 접근제어

에 장애가 발생할 경우를 대비하여 보조 서버가 이중 해쉬 처리를 담당하여 속성 정보를 가진 사용자의 헬스케어 정보에 대한 권한에 따라 사용자의 의료정보에 손쉽게 접근할 수 있기 때문에 나타난 결과이다. 반면, 기존 기법은 IoT 장치의 동기화 없이 서버가 FIFO 방식으로 사용자의 헬스케어 정보를 저장, 분석, 피드백하기 때문에 디바이스 수가 증가할수록 서버에서 IoT 장치를 처리하는 비율은 점점 감소하였다. 그러나, 감소 비율이 IoT 장비 수 증가에 따라 0.1%~0.3정도밖에 차이가 나지 않아 전체적으로는 감소차이가 크게 나타나지 않았다.

4.2 서버의 오버헤드

[Fig. 5]은 IoT 기반의 모바일 헬스케어 서비스를 제공하는 서버의 오버헤드를 나타내고 있다. [Fig. 4]의 결과, 헬스케어 센서 정보 별로 속성 값을 부여하여 사용자의 프라이버시를 계층적으로 통합 관리하는 제안 기법의 서버 오버헤드가 평균 9.9% 낮게 나타났다. 이 같은 결과는 사용자의 헬스케어 정보를 안전하게 처리, 보관, 저장할 수 있도록 헬스케어 센서 정보 별로 속성 값을 부여하여 센서가 탑재된 장비(e.g. 팔찌, 목거리 등)와 휴대폰을 통해서 사용자의 헬스케어 정보를 실시간으로 확인하여 신속하게 대응할 수 있기 때문에 나타난 결과이다. 특히, 제안 기법은 IoT 장치에서 수집한 헬스케어 정보를 일일이 모두 처리하지 않고 해당 헬스케어 정보의 속성에 따라 계층적으로 분리 처리 분석하기 때문에 기존기법보다 서버의 오버헤드가 낮게 나타났다.



[Fig. 5] Overhead of Server

5. 결론

최근 IoT 기술을 기반으로 의료 서비스를 사용자에게 손쉽게 제공하기 위한 시도가 병원을 중심으로 증가하고 있다. 본 논문에서는 IoT 기반의 웨어러블 장비를 이용한 사용자의 헬스케어 정보를 서버에 전달할 때 제 3자로부터 사용자의 헬스케어 정보를 안전하게 처리할 수 있는 사용자 프라이버시 보호 모델을 제안한다. 제안 모델은 헬스케어 센서 정보 별로 속성 값을 부여하여 사용자의 프라이버시를 계층적으로 통합 관리한다. 또한, 제안 모델은 센서가 탑재된 장비(e.g. 팔찌, 목거리 등)와 휴대폰을 이용하여 사용자의 헬스케어 정보를 확인하고 처리할 수 있다. 향후 연구에서는 본 연구의 보안 문제점 및 해결 방안에 대해서 연구를 수행할 계획이다.

ACKNOWLEDGMENTS

This work was supported by the Security Engineering Research Center granted by the Ministry of Trade, Industry and Energy.

REFERENCES

[1] T. Y. Kim, S. K. Y. J. J. Jung and E. J. Kim, “Multi-Hop WBAN Construction for Healthcare IoT Systems”, 2015 International Platform Technology and Service(PlatCon), pp. 27-28, Jan. 2015.

[2] Y. S. Jeong, “An Efficient IoT Healthcare Service Management Model of Location Tracking Sensor”, Journal of Digital Convergence, Vol. 14, No. 3, pp. 261-267, Mar. 2016.

[3] C. Doukas and I. Maglogiannis, “Bringing IoT and Cloud Computing towards Pervasive Healthcare”, 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp.922-926, July. 2014.

[4] B. Zhang, X. W. Wang, M. Huang, “A data replica placement scheme for cloud storage under healthcare IoT environment”, 2014 11th International Conference

on Fuzzy Systems and Knowledge Discovery (FSKD), pp. 542-547, Aug. 2014.

[5] Y. S. Jeong, "Design of Prevention Model according to a Dysfunctional of Corporate Information," Journal of Convergence Soceity for SMB, Vol. 6, No. 2, pp. 11-17, Jun. 2016.

[6] Y. S. Jeong, "Tracking Analysis of User Privacy Damage using Smartphone", Journal of Convergence Society for SMB, Vol. 4, No. 4, Dec. 2014.

[7] Y. S. Jeong, "Design of Security Model for Service of Company Information," Journal of Convergence Soceity for SMB, Vol. 2, No. 2, pp. 43-49, Nov. 2012.

[8] J. T. Park, S. M. Cheon and S. J. Go, "Things Internet-based Healthcare Services and Platform Trends", Information & Communications Magazine, Vol. 3, No. 12, pp. 25-30, Dec. 2014.

[9] Y. S. Jeong, "Secure biometric information delivery scheme of implantable device using code-division multiplexing method", Journal of Digital Convergence, Vol. 14, No. 3, pp. 235-241, Mar. 2016.

[10] Y. S. Jeong, "A Study of An Efficient Clustering Processing Scheme of Patient Disease Information for Cloud Computing Environment", Journal of Convergence Society for SMB, Vol. 6, No. 1, pp. 33-38, Mar. 2016.

[11] Y. S. Jeong, "An Efficient Hospital Service Model of Hierarchical Property information classified Bioinformatics information of Patient", Journal of Convergence Society for SMB, Vol. 5, No. 4, pp. 11-16, Dec. 2015.

[12] V. Shnayder, B. Chen, K. Lorincz, T. R. F. F. Jones, and M. Welsh, "Sensor networks for medical care," Proc. 3rd Int. Conf. Embed. networked Sens. Syst. SenSys OS, no. June, p. 314,2005.

[13] Y. S. Jeong, "Medical Information Management Scheme of Healthcare Service Patient through 2-way Access Control", Journal of Digital Convergence, Vol. 14, No. 7, pp. 185-191, Jul. 2016.

[14] Z. A. Khattak, S. Sulaiman and J. A. Manan, "A study on threat model for federated identities in federated identity management system", 2010 International Symposium in Information Technology(ITSim), Vol. 2, pp. 618-623, 2010.

[15] H. Gao, J. Yan and Y. Mu, "Dynamic Trust Model for Federated Identity Management", 2010 4th International Conference on Network and System Security(NSS), pp. 55-61, 2010.

[16] Y. Zhou, Z. Cao, and R. Lu, "Provably secure proxy-protected signature schemes based on factoring", Appl. Math. Comput. Vol. 164, No. 1, pp. 83-98, 2005.

[17] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation", Proc. Third ACM Conf. on Computer and Communications Security, pp. 48-57, 1996.

[18] R. Lu, Z. Cao and Y. Zhou, "A simple efficient proxy-protected signature scheme based on factoring", Comp. Stand. Inter., withdrawn, 2004.

[19] Y. S. Jeong, K. H. Han and S. H. Lee, "Access Control Protocol for Privacy Guarantee of Patient in Emergency Environment", Journal of Digital Convergence, Vol. 12, No. 7, Jul. 2014.

정 윤 수(Jeong, Yoon Su)

- 2000년 2월 : 충북대학교 전자계산학과 이학석사
- 2008년 2월 : 충북대학교 전자계산학과 이학박사
- 2009년 8월 ~ 2012년 2월 : 한남대학교 산업기술연구소 전임연구원
- 2012년 3월 ~ 현재 : 목원대학교 정보통신융합공학부 조교수
- 관심분야 : 유·무선통신 보안, 정보보호, 센서 네트워크, IoT, 이동통신, 암호이론,
- E-Mail : bukmunro@mokwon.ac.kr