Journal of Convergence for Information Technology
Vol. 9. No. 11, pp. 8-14, 2019
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2019.9.11.008

IoT 사용자의 빅데이터 정보를 안전하게 보호하기 위한 IoT 정보 보안 모델

정윤수[1], 윤덕병[2], 신승수[3*]
[1]목원대학교 정보통신융합공학부 교수, [2]동명대학교 경영학과 교수, [3]동명대학교 정보보호학과 교수

An IoT Information Security Model for Securing Bigdata Information for IoT Users

Yoon-Su Jeong[1], Deok-Byeong Yoon[2], Seung-Soo Shin[3*]
[1]Professor, Department of information Communication Convergence Engineering, Mokwon University
[2]Professor, Department of Business, Tongmyong University
[3]Professor, Department of Information Security, Tongmyong University

요 약 컴퓨터 기술의 발전으로 인하여 IoT 기술은 산업, 경제, 의료서비스 및 교육 분야에서 다양하게 사용되고 있다. 그러나, IoT 장비를 통해 처리되는 멀티미디어 정보는 아직까지 애플리케이션 분야에서 무결성과 기밀성 문제가 큰 이슈 중 하나로 손꼽히고 있다. 본 논문에서는 IoT 장비를 통해 처리되는 사용자의 빅데이터 정보에 안전성을 보장하기 위한 스테가노그래피 기반의 IoT 사용자의 빅데이터 보호 모델을 제안한다. 제안 모델은 사용자의 동의 없이 IoT 장비를 통해 수집된 사용자의 빅데이터 정보를 불법적으로 악용되는 것을 예방하는 것이 목적이다. 제안 모델은 IoT 사용자의 빅데이터에 서명과 인증 정보를 하이브리드 암호 방식으로 사용한다. 제안 모델은 IoT를 통해 수집된 사용자의 빅데이터에 대한 무결성 및 기밀성을 보장하는 특징이 있다. 또한, IoT 사용자의 빅데이터는 스테가노그래피 기반의 암호 처리 기법을 사용하여 사용자의 서명 정보를 암호화하였기 때문에 제 3자가 사용자의 정보를 악의적으로 사용되지 못한다.

주제어 : 스테가노그래피, IoT, 사용자 정보, 빅데이터, 정보 보호

Abstract Due to the development of computer technology, IoT technology is being used in various fields of industry, economy, medical service and education. However, multimedia information processed through IoT equipment is still one of the major issues in the application sector. In this paper, a big data protection model for users of IoT based IoT is proposed to ensure integrity of users' multimedia information processed through IoT equipment. The proposed model aims to prevent users' illegal exploitation of big data information collected through IoT equipment without users' consent. The proposed model uses signatures and authentication information for IoT users in a hybrid cryptographic method. The proposed model feature ensuring integrity and confidentiality of users' big data collected through IoT equipment. In addition, the user's big data is not abused without the user's consent because the user's signature information is encrypted using a steganography-based cryptography-based encryption technique.

Key Words : Steganography, IoT, User information, Bigdata, Information security

*This Research was supported by the Tongmyong University Research Grants 2018(2018A045-1).

*Corresponding Author : Seung-Soo Shin(shinss@tu.ac.kr)

Received October 1, 2019
Revised October 30, 2019
Accepted November 20, 2019
Published November 28, 2019

1. 서론

최근 IoT 기술은 스마트 홈을 중심으로 다양한 학문 분야에서 큰 이슈가 되고 있다. IoT 기술은 빅데이터와 관련된 연구가 증가하면서 IoT 장비를 통해 수집되는 정보의 양이 점점 증가하고 있다[1-3]. 특히, IoT 기술은 빅데이터와 융합되면서 의료서비스, 건강관리 서비스, 스마트 홈 서비스 등을 중심으로 기술발전에 따라 부분적 또는 장기적으로 대체 가능한 분야가 만들어지고 있다[4].

IoT 서비스는 국내·외 국가 경쟁력 및 상호 운영성 등을 통해 시장 규모가 확장되고 있으며 3가지 측면(경제적 측면, 기술 표준화를 통한 기술적 측면, 표준 인터페이스 및 표준 사용법을 통한 사용자 보호 측면 등)에서 비용과 관련된 중요한 의미를 내포하고 있다[5,6].

최근 IoT 서비스는 빅데이터와 융합되면서 국·내외적으로 많은 분야에서 활용되고 있다. 국내 통신사 LG 유플러스는 홈 IoT(도어락, 전용 플러그, IoT 음성 제어 등)를 마케팅에 활용되고 있다. 다른 국내 통신사 올래 KT는 최근 기가 지니를 출시하여 IoT 허브와 연동이 가능한 홈 IoT 기기를 조작(음성 명령어를 통한 불 켜기 및 공기청정기 작동)하도록 하였다. 핀란드의 베딧사는 사용자의 수면 활동을 측정할 수 있는 '베딧'이라는 수면 추적기를 개발하였다. 필립스사는 칫솔에 위치, 압력, 이동경로 등을 처리할 수 있는 스마트 칫솔을 개발하였다.

본 논문에서는 사회적으로 대두되고 있는 IoT 장치의 빅데이터 정보를 안전하게 보호할 수 있는 스테가노그래피 기반의 IoT 사용자의 빅데이터 보호 모델을 제안한다. 제안 모델은 IoT 장치를 이용하여 다양한 빅데이터 정보를 처리할 뿐만 아니라 빅데이터 정보처리의 질을 향상시키고 있다. 제안 모델은 IoT 장치에서 수집되는 빅데이터를 바탕으로 손쉽게 사용자의 개인정보를 보호할 수 있도록 스테가노 그래피를 사용한다. 제안 모델은 다음과 같은 2가지 목표를 가지고 IoT 장치에서 처리되는 빅데이터의 효율성을 향상시키고 있다.

첫째, 제안 모델은 IoT 장치에서 수집된 빅데이터를 손쉽게 처리할 수 있도록 빅데이터의 확률 정보를 연계처리함으로써 IoT 사용자의 빅데이터에 대한 접근성을 향상시켰다.

둘째, 제안 모델은 빅데이터 정보의 유사도에 따라 계층적 구조로 그룹핑 함으로써 IoT 사용자의 빅데이터의 정확성을 보장받는다.

제안 모델은 IoT 장치를 이용하는 사용자의 빅데이터를 빠르게 처리할 수 있도록 빅데이터에 대한 유사도 검사를 수행한다. 또한, 제안 모델은 우선순위에 따라 빅데이터의 그룹 크기가 정해져서 상위계층에 포함된 빅데이터가 하부계층의 빅데이터를 포함하도록 다양한 속성 정보를 세분화하여 빅데이터의 정확도를 향상시킨다.

이 논문의 구성은 다음과 같다. 2장에서는 IoT 기술과 빅데이터와 관련된 기존 연구에 대해서 알아본다. 3장에서는 스테가노그래피 기반의 IoT 사용자의 빅데이터 보호 모델을 제안하고, 4장에서는 제안 모델을 평가하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

IoT 장치에서 발생되는 데이터를 이용하는 기술들은 현재 다양하게 연구되고 있으며 가장 대표적인 연구를 정리하면 Table 1과 같다.

Table 1. Comparisons for previous scheme vs. proposed scheme

Scheme	Advantage	Disadvantage
[7]	Used in most applications	Pre-process relevant information for application availability
[8]	Use watermarking technique to process credentials	Security-related issues are not Solving
[10]	It deals with data related to various issues in the social and economic sectors	Security algorithms related to authentication and encryption are not implemented
[13]	Performs authentication behavior associated with DoS attacks through the user's unique identification	Vulnerable in Security Attack
[14]	Improves safety in authentication and data access control	Limit access to parameters using ID and random values
[16]	Access data shared by all users	Mutual authentication is not smooth due to high constraints on access to collected IoT data

J. G. KO et al. 기법은 IoT 장치를 이용하여 의료데이터와 연관된 생화학적 정보를 분석하기 위한 기법을 제안하였다[7]. 이 기법은 대부분의 애플리케이션에서 사용할 수 있도록 관련 정보들을 처리할 수 있도록 한 것이 특징이다.

S. C. Rathi et al. 기법은 IoT 장치를 통해 수집된

개인 정보를 지원하기 위한 인증 방법을 제안하였다[8]. 이 기법은 인증 정보처리를 위해서 워터마킹 기법을 사용한 것이 특징이다. 그러나, 이 기법은 IoT 정보를 전송할 때 보안과 관련된 문제를 해소하지 못한 것이 단점이다.

G. Virone et al. 기법은 IoT 장치를 의료 서비스와 관련된 새로운 프레임워크를 제안하였다[9].

Al Ameen et al. 기법은 IoT 보안 및 개인 정보보호와 관련된 애플리케이션의 위험 범주를 분류하였다[10]. 이 기법은 사회·경제 분야의 다양한 이슈들과 관련된 데이터를 다루고 있지만, 인증 및 암호화와 관련된 보안 알고리즘이 구현되어 있지 않은 것이 문제이다[11,12].

R. Fan et al. 기법은 IoT 장치를 이용한 2계층의 인증 기법을 제안하고 있다[13]. 이 기법은 IoT 의료 정보와 관련된 DoS 공격과 관련된 인증 동작을 사용자의 고유 식별을 통해 수행하고 있지만 여전히 보안 공격에 취약하다.

N. Gonzalez et al. 기법은 IoT 의료 정보를 안전하게 전달하기 위한 접근 제안 모델을 제안하였다 [14]. 이 기법은 매개변수를 ID와 무작위 값을 사용하여 접근을 제한하고 있기 때문에 인증과 데이터 접근 제어에 안전성을 향상시킨 것이 특징이다[15].

Q. A. Kester et al. 기법은 데이터의 접근을 모든 사용자들이 공유할 수 있는 검증 방법을 제안하였다[16]. 그러나, 이 기법은 수집된 IoT 데이터의 접근에 제약 조건이 높아 상호 인증이 원활하지 못하다.

3. 스테가노그래피 기반의 IoT 사용자 빅데이터 보호 모델 설계

3.1 IoT 사용자의 빅데이터 보호

IoT 장치에서 수집된 빅데이터 정보를 이용하여 IoT 사용자의 무결성을 보장하기 위한 스테가노그래피 기반 IoT 사용자의 빅데이터 보호 모델을 제안한다. 제안 모델은 IoT 사용자의 동의 없이 제 3자가 불법적으로 악용하는 것을 예방하고 있다. 제안 모델은 IoT 사용자의 빅데이터 정보 중 서명과 인증 정보를 스테가노그래피를 통해 하이브리드 암호방식을 사용한다. 이 같은 이유는 IoT 사용자의 빅데이터가 제3자로부터 안전하게 처리할 수 있는 기밀성을 보장하기 때문이다. 또한, IoT 사용자의 빅데이터는 스테가노그래피 기반의 암호처리 기법을 사용하기 때문에 IoT 사용자의 서명 정보를 동의 없이 불법적으로 악용하는 것을 예방한다.

제안 모델은 IoT 장비로부터 수집된 1개 이상의 빅데이터 정보(개인 신상정보, 위치정보 등)를 안전하게 처리하기 위해서 3단계(수집단계, 전송단계, 분석단계)로 동작된다. Fig. 1은 제안 모델에서 IoT 사용자의 빅데이터 정보를 관리자에게 전달하기 위한 3단계의 동작 과정을 보여주고 있다.

수집단계는 IoT 사용자의 빅데이터 정보를 첨단 장비를 통해 수집하는 단계이다. 전송단계는 Cellular Networks와 WLAN를 통해 IoT 빅데이터 정보를 안전하게 전달하는 단계이다. 마지막으로 분석단계는 전송된 IoT 사용자의 빅데이터 정보를 분석하는 단계이다.

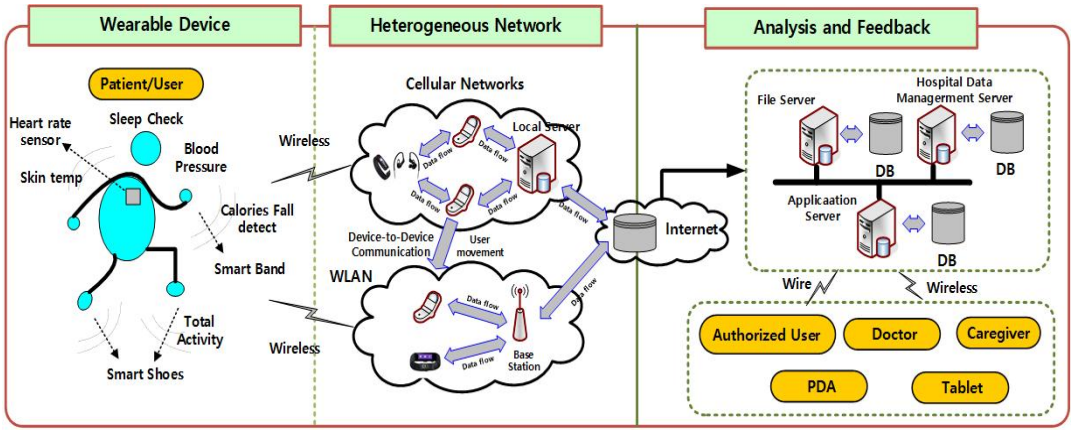

Fig. 1. Transmission process of multimedia information

수집단계에서는 IoT 장치의 데이터를 수집하기 위한 다양한 센서(Heart rate 센서, Sleep Clock 센서, Blood Pressure 센서, Activity 센서, Smart Shoes 센서 등)들로 구성되어 있다. 전송단계에서는 IoT 장치로부터 생성된 다양한 센서 들을 관리 서버에게 전송하기 위해 다양한 장치(스마트폰, 태블릿, 게이트웨이, 중간 서버 등)들이 필요하다. 분석단계에서는 IoT 데이터를 분석하기 위한 서버, 데이터베이스 및 애플리케이션 등이 필요하다.

3.2 IoT 사용자의 빅데이터 정보 생성

이 단계는 IoT 장비로부터 수집된 1개 이상의 빅데이터 정보(개인 신상정보, 위치정보 등)를 안전하게 처리하기 위한 수집단계로써, IoT 사용자의 빅데이터 정보 생성 과정은 첨단 의료 장비를 통해 수집된 IoT 사용자의 빅데이터 정보를 관리자 및 제 3자에게 IoT 사용자의 빅데이터 정보를 안전하게 전달하기 위한 무결성 검증의 전 단계이다. 이 단계에서는 IoT 사용자의 빅데이터 정보의 무결성을 검증하기 위해서 IoT 사용자의 중요 정보를 N-1차 다항식을 사용한다. N-1차 다항식을 사용하는 이유는 스테가노그래피를 이용하여 식 (1)처럼 암호화된 IoT 빅데이터의 비밀 정보를 샘플링하기 때문이다.

$$IBD_x=\begin{cases} i_1+i_2x^1+\cdots+i_nx^{n-1}, \text{if } i,n>1 \\ 1 \qquad\qquad\qquad\qquad\quad , otherwise \end{cases} \tag{1}$$

식 (1)처럼 분산 배치할 IoT 사용자의 비밀 정보 IBD_x에 스테가노그래피 정보를 생성하기 위해서 식 (2)처럼 IoT 사용자의 정보에 위장할 정보를 생성한다.

$$s_n = IBD_x \bmod s \tag{2}$$

스테가노그래피 기반의 비밀정보 $\sum_{i=1}^{n} s_n$은 스테가노그래피 기법을 이용하여 암호화된 IoT 빅데이터 정보를 분산처리 하여 각 정보가 식별될 수 있도록 은닉정보 $s_1+s_2+\cdots+s_n$을 중첩한다. 은닉정보를 중첩하는 이유는 스테가노그래피 기반의 비밀정보가 무손실로 복원하기 위해서이다.

3.3 암 · 복호화 키 생성

이 단계는 IoT 장비로부터 수집된 1개 이상의 빅데이터 정보(개인 신상정보, 위치정보 등)를 안전하게 처리하기 위한 전송단계로써, IoT 사용자의 빅데이터 정보를 암·복호화기 위해서 사용되는 키는 식 (3)~식 (4)을 통해 공개키와 개인키를 생성한다.

$$x_i^{n[i]} = \begin{cases} x_i^0, \text{if } n[i]=0 \\ x_i^1, \text{if } n[i]=1 \end{cases} \tag{3}$$

$$PK_{i+1}^{n} = h(x_{i+1}^{n[i]}) = \begin{cases} PK_{i+1}^{n[i]} = h(x_{i+1}^{n[i]}), \text{if } n[i]=0 \\ PK_{i+1}^{n[i]} = h(x_{i+1}^{n[i]}), \text{if } n[i]=1 \end{cases} \tag{4}$$

식 (3)은 IoT 사용자의 빅데이터에 대한 무결성 검증을 위해서 이진 값에 의해 생성된 랜덤 수 x_1^0, x_1^1 을 식 (4)에 대응 되도록 적용하고 있다. 이 같은 과정을 거치는 이유는 IoT 사용자의 빅데이터의 무결성 보장과 제 3자의 악의적인 접근을 사전에 예방하기 위해서이다.

3.4 IoT 사용자의 빅 데이터 검증 과정

이 단계는 IoT 장비로부터 수집된 1개 이상의 빅데이터 정보(개인 신상정보, 위치정보 등)를 안전하게 처리하기 위한 분석단계로써, 이 과정은 관리자에게 전달된 IoT 사용자의 빅데이터 정보를 검증하는 과정이다. 관리자는 IoT 사용자의 빅데이터 정보를 전달 받은 후 IoT 사용자의 비밀 정보 IBD_X을 확인한다. 관리자는 IoT 사용자의 빅데이터 정보에 포함된 스테가노그래피 정보를 $s_n = IBD_x \bmod s$ 처럼 계산하여 분산 암호화된 IoT 사용자의 빅데이터 정보를 식별할 수 있도록 $s_n^{'} = s_n - IBD_x$을 계산한다. IoT 사용자의 비밀정보에 포함된 스테가노그래피 기반의 비밀정보 $\sum_{i=1}^{n} s_n$에 대한 은닉정보 $s_1+s_2+\cdots+s_n$을 확인함으로써 IoT 사용자의 빅데이터를 검증한다.

4. 평가

4.1 환경 설정

제안 모델에서 IoT 사용자의 빅데이터 정보는 Fig. 2

와 같은 아두이노와 같은 장치를 사용하였다. Fig. 2처럼 제안 모델에서는 IoT 사용자의 빅데이터 5개를 사용하여 사용자의 각 신상 정보를 송·수신할 수 있도록 구축하여 성능을 분석하였다. 성능평가의 비교분석을 위한 기존연구는 [4]를 기반으로 제안 모델과 비교평가를 수행하였다.

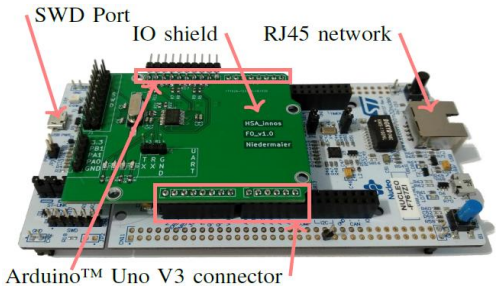

Fig. 2. IoT Device for simulation

4.2 성능 평가

4.2.1 효율성

Fig. 3처럼 효율성에 대한 성능평가에서는 IoT 사용자의 빅데이터 정보를 수집하기 위해서 첨단 장비를 사용할 때 발생하는 빅데이터 처리를 평가하였다. 효율성 평가에서는 IoT 사용자의 빅데이터를 사용자의 신상 정보 수에 따라 IoT 사용자의 빅데이터를 수집 및 조사 분석한 결과를 이용하였다. 효율성의 성능평가에 따라 IoT 사용자의 신상 정보 수에 따른 IoT 사용자의 빅데이터 처리에 대한 효율성은 기존 모델보다 6.5% 높은 결과를 얻었다. 이 같은 결과는 IoT 사용자의 신상 정보의 관리 및 접근 권한에 따라 빅데이터의 처리 방법이 달라지기 때문에 나타난 결과이다.

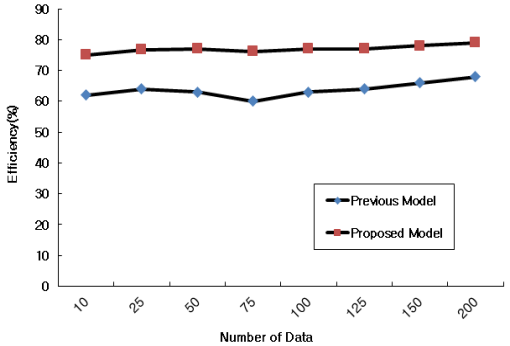

Fig. 3. Efficiency according to the degree of information collected

4.2.2 정확도

Fig. 4처럼 정확도에 대한 성능평가는 첨단 장비들을 통해 수집된 IoT 사용자의 빅데이터 정보 중 IoT 사용자의 신상 정보, IoT 사용자의 환경에 따라 수집된 정보의 추출 정도에 따른 정확도를 평가하였다. 정확도에 대한 평가에서는 IoT 사용자의 빅데이터 정보 수집이 정확하게 분석하는 비율이 그렇지 않은 경우보다 평균 7.7% 높게 나타났다. 이 같은 결과는 제안 모델이 첨단 장비를 통해 수집된 정보들 간 빅데이터 정보의 애매성을 보완하기 위해서 쌍대비교 행렬과 스테가노그래피 기법을 사용하였기 때문에 나타난 결과이다. 또한, IoT 사용자의 빅데이터를 분산 처리하여 암·복호하는 과정이 추가적으로 적용하였기 때문에 나타난 결과이다.

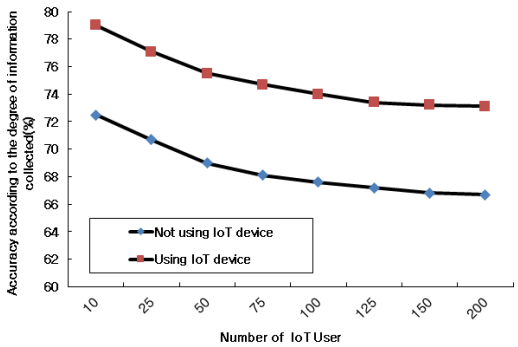

Fig. 4. Accuracy according to the degree of information collected

4.2.3 무결성

제안 모델과 기존 모델과의 IoT 사용자의 빅데이터 정보의 무결성을 체크한 결과 Table 2처럼 6개 항목(Data dynamics, public auditability, Server comp. complexity. Verifier comp. complexity, Encryption comp. complexity, Verifier storage complexity)의 평가 결과가 나왔다. Table 2처럼 제안 모델은 기존 모델에 비해 N-1차 다항식을 사용하여 사용자의 비밀 정보를 분산 처리하도록 샘플링 하는 과정을 사용하였기 때문에 IoT 사용자의 비밀정보에 삽입된 빅데이터 정보를 정확하게 알지 못한다. 또한, IoT 사용자의 빅데이터 정보에 은닉 정보를 중첩하여 사용하기 때문에 빅데이터가 손실 없이 복원되었다. 또한, 제안 모델은 IoT 사용자의 빅데이터가 병합 처리되기 때문에 O(logn)와 같은 검증 비교/저장 복잡도 나타난다.

Table 2. Comparisons for Integrity of previous scheme vs. proposed scheme

Scheme	Data dynamics	Public auditability	Server comp. complexity	Verifier comp. complexity	Encryption comp. complexity	Verifier storage complexity
Previous Scheme	No	Low	O(nlogn)	O(1)	O(logn)	O(1)
Our Scheme	Yes	High	O(logn)	O(logn)	O(1)	O(logn)

5. 결론

최근 IoT 기술이 다양한 분야에서 관심을 받고 있는 가운데 빅데이터와 관련된 IoT 기술 연구가 증가하고 있다. 특히, IoT 기술은 국내·외 국가 경쟁력 및 상호 운영성을 향상시키기 위해서 의료 서비스, 건강관리 서비스, 스마트 홈 서비스 등을 중심으로 연구가 만들어지고 있다. 본 논문에서는 IoT 장치에서 발생하는 빅데이터 정보를 안전하게 보호할 수 있는 스테가노그래피 기반의 IoT 사용자의 빅데이터 보호 모델을 제안하였다. 제안 모델은 IoT 장치에서 수집된 빅데이터를 손쉽게 처리할 수 있도록 빅데이터의 확률 정보를 연계 처리하여 빅데이터의 접근성을 향상시켰다. 또한, 제안 모델은 빅데이터 정보의 유사도에 따라 계층적 구조로 그룹핑 함으로써 IoT 사용자의 빅데이터의 정확성을 보장받도록 하였다. 성능평가 결과, 효율성은 IoT 사용자의 신상 정보 수에 따른 IoT 사용자의 빅 데이터 처리에 대한 효율성을 기존 모델보다 6.5% 높은 결과를 얻었다. 정확도는 IoT 사용자의 빅데이터 정보 수집에 대한 정확도 분석이 평균 7.7% 높게 나타났다. 향후 연구에서는 기존 연구를 기반으로 이질적인 클라우드 환경에서 IoT 사용자의 빅데이터 정보를 효율적으로 분석하는 방법을 연구할 계획이다.

REFERENCES

[1] S. M. R. Islam, D. Kwak, M. Kabir, M. Hossain &. Kwak. (2015). The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access, 3,* 678-708.

[2] L. Catarinucci, D. de Donno, L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi & L. Tarricone. (2015). An IoT-Aware Architecture for Smart Healthcare Systems. *IEEE Internet of Things Journal, 2(6)*, 515-526.

[3] S. K. Datta, C. Bonnet, A. Gyrard, R. P. Ferreira da Costa & K. Boudaoud. (2015). Applying Internet of Things for personalized healthcare in smart homes, *WOCC*, 164-169.

[4] H. Samani & R. Zhu. (2016). Robotic Automated External Defibrillator Ambulance for Emergency Medical Service in Smart Cities. *IEEE Access, 4*, 268-283.

[5] J. J. Yang, J. Q. Li & Y. Niu. (2015). A hybrid solution for privacy preserving medical data sharing in the cloud environment. *Future Generation Computer Systems, 43(44)*, 74-86.

[6] X. B. Li & L. Z. Lu. (2015). General Construction Method of Multilength Optical Orthogonal Codes With Arbitrary Cross-Correlation Constraint for OCDMA Multimedia Network. *Journal of Optical Communications and Networking, 7(3)*, 156-163.

[7] J. G. Ko., C. Lu., M. B. Srivastava., J. A. Stankovic., A. Terzis. & M. Welsh. (2010). Wireless sensor networks for healthcare. *Proceedings of the IEEE, 98(11),* 1947-1960.

[8] S. C. Rathi & I. Technology. (2012) Medical Image Authentication through Watermarking Preserving ROI. *Health Information - An International Journal, 2*, 292-295.

[9] G. Virone., A, Wood. L. Selavo., Q. Cao., L. Fang., T. Doan. & J. A. Stankovic. (2006). An Advanced Wireless Sensor Network for Health Monitoring. *Transdisciplinary Conference on Distributed Diagnosis and Home Healthcare (D2H2),* 2-5.

[10] M. AI Ameen., J. Liu & K. Kwak. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems, 36(1)*, 93-101.

[11] T. Yang, D. Mu, W. Hu & H. Zhang. (2014). Energy-efficient border intrusion detection using wireless sensors network. *EURASIP Journal on Wireless Communications and Networking, 1,* 46.

[12] D. Liu, T. Song & Y. Dai. (2005). Isomorphism and generation of Montgomery-form elliptic curves suitable for cryptosystems. *Tsinghua Science and Technology,* 10(2), 145-151.

[13] R. Fan, D. J. He, X. Z. Pan & L. D. Ping. (2011). An efficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks.

Journal of Zhejiang University-Science C-Computers & Electronics, 12(7), 550-560.

[14] N. Gonzalez, C. Miers, F. Redigolo, T. Carvalho., M. Simplicio, M. Naslund & M. Pourzandi. (2011). A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing. *2011 IEEE Third International Conference on Cloud Computing Technology and Science,* 231-238.

[15] G. Garkoti, S. K. Peddoju & R. Balasubramanian. (2014). Detection of insider attacks in cloud based e-healthcare environment. *Proceedings - 2014 13th International Conference on Information Technology(ICIT 2014),* 195-200.

[16] Q. A. Kester, L. Nana, A. C. Pascu, S. Gire, J. M. Eghan & N. N. Quaynor. (2015). A Security Technique for Authentication and Security of Medical Images in Health Information Systems. *Proceedings - 15th International Conference on Computational Science and Its Applications(ICCSA 2015),* 8-13.

정 윤 수(Yoon-Su Jeong) [정회원]

· 1998년 2월 : 청주대학교 전자계산학과 학사
· 2000년 2월 : 충북대학교 전자계산학과 석사
· 2008년 2월 : 충북대학교 전자계산학과 박사
· 2012년 3월 ~ 현재 : 목원대학교 정보통신공학과 조교수
· 관심분야 : 유·무선 통신 보안, 정보보호, 바이오인포매틱, 헬스케어, 빅데이터, 클라우드 컴퓨팅
· E-mail : bukmunro@gmail.com

윤 덕 병 (Deok-Byeong Yoon) [정회원]

· 1985년 2월 : 성균관대학교 세무학과 석사(경영학석사)
· 1998년 2월 : 동의대학교 법학과 (법학박사)
· 1994년 3월 ~ 현재 : 동명대학교 경영학과 교수
· 관심분야 : 정보보호법, 전자상거래법, ICT 법률
· E-mail : dbjob@naver.com

신 승 수 (Seung-Soo Shin) [정회원]

· 2001년 2월 : 충북대학교 수학과 이학박사
· 2004년 2월 : 충북대학교 컴퓨터공학과 공학박사
· 2005년 3월 ~ 현재 : 동명대학교 정보보호학과 교수
· 관심분야 : 헬스케어 보안, 빅 데이터, 블록체인, 정보보호
· E-mail : shinss@tu.ac.kr