Journal of The Korea Society of Computer and Information
Vol. 21 No.1, pp. 85-90, January 2016

www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2016.21.1.085

A Study on the Security Technology of Real-time Biometric Data in IoT Environment

Yoon-Hwan Shin *

Abstract

In this paper, the biometric data is transmitted in real time from the IoT environment is runoff, forgery, alteration, prevention of the factors that can be generated from a denial-of-service in advance, and the security strategy for the biometric data to protect the biometric data secure from security threats offer. The convenience of living in our surroundings to life with the development of ubiquitous computing and smart devices are available in real-time. And is also increasing interest in the IOT. IOT environment is giving the convenience of life. However, security threats to privacy also are exposed for 24 hours. This paper examines the security threats to biological data to be transmitted in real time from IOT environment. The technology for such security requirements and security technology according to the analysis of the threat. And with respect to the biometric data transmitted in real time on the IoT environment proposes a security strategy to ensure the stability against security threats and described with respect to its efficiency.

▸ Keyword : IoT, Biological Data, Security, Ubiquitous Computing

I. Introduction

의학의 발달로 인간의 수명을 계속해서 늘어나고 있으며 모든 사람들이 건강한 생활에 대한 관심도가 점차 높아가고 있다. 최근에는 사물인터넷 환경에서의 건강관련 정보들이 홍수처럼 쏟아지고 있으며 이를 기반으로 개인들도 본인의 건강한 정보와 상식에 대한 노하우를 가지게 되었다. 사물인터넷 기술은 실시간 생체 데이터와 같은 빅데이터와 클라우드 기술 등 다양한 기술과 융/복합되어 생활공간 속에서 사물과 사물 또는 사물과 사람, 사람과 사람의 연결을 통하여 인간의 새로운 가치를 제공하는 것을 목표로 동적 연결이 가능하게 함으로써 진정한 유비쿼터스 환경을 실현 시킬 수 있는 기술이라고 설명했다[1-4].

의학신문 2016년 1월 5일자에 의하면 건강보험심사평가원에서 전자의무기록시스템(EMR)의 효율성을 강화하기 위해 표준 EMR 승인체제 등 4개의 대안을 제시했다[5].

건강보험심사평가원에서 제시한 4개의 대안 중에서 본 논문에서 고찰하고자 하는 대안은 “표준 EMR 승인체제 모형”에 대한 내용이다. 이 대안은 공적기관에서 인증된 표준 EMR 시스템은 용어, 서식, 환자진료정보교류, 시스템 보안성, 환자정보 보호 등에 대한 기본적인 요건을 갖춘 것으로 검증을 통과한 경우에 한해 ‘표준 EMR 시스템’으로 사용하도록 하는 방안으로 Fig. 1과 같이 나타냈다. Fig. 2는 의료기관 및 청구솔루션 개발회사들은 시장에서 자유롭게 맵핑할 수 있는 표준과 각 의료 SW기관의 시스템에 적용될 수 있도록 표준 프레임워크 개발에 관한 내용이다. 이렇게 표준안을 제정하고자 하는 이유는 유·무선 통신망을 통하여 개인의료기록 내용이 전송되고 관리되기 때문이다.

• First Author: Yoon-Hwan Shin, Corresponding Author: Yoon-Hwan Shin
*Yoon-Hwan Shin(cskisa@naver.com), Technology Commercialization Advisory Committee member for Technical Support Division of KIAT, Korea Institute for Advancement of Technology
• Received: 2016. 01. 20, Revised: 2016. 01. 26, Accepted: 2016. 01. 28.

유·무선 네트워크는 사물인터넷 서비스가 지원될 수 있는 환경을 제공하게 되었다. 사물 인터넷 환경에서에서는 각 객체 간 상호 정보를 자유롭게 교환할 수 있는 환경 구축이 가능하므로 새로운 서비스가 제공될 때 발생할 수 있다. 그렇기 때문에 불법적인 접근과 보안에 위협되는 요인들을 찾아서 제거하기란 쉽지 않다. 이러한 이유로 사물인터넷 환경은 유·무선 네트워크에서 발생될 수 있는 생체 데이터의 유출, 복제, 위조, 변조 등의 보안문제가 대두되고 있다. 그렇기 때문에 사물인터넷 서비스 환경에서는 복합적이고 체계적인 보안 전략이 요구된다. 따라서 본 논문에서는 사물 인터넷 서비스 환경에서 실시간 전송되는 생체 데이터를 위협요인들로부터 보호하기 위한 보안전략을 제안한다.

본 논문의 구성은 2장에서 사물인터넷 환경에서 실시간으로 전송되는 생체 데이터의 수집과정에 대해서 기술하고 3장에서는 생체 데이터의 보안을 위협할 수 있는 요인들에 대해서 분석한다. 4장에서는 사물인터넷 환경에서 요구되는 보안기술에 대해서 기술하고 5장에서는 실시간 생체 데이터에 대한 보안전략을 제안한다. 마지막으로 6장에서는 본 논문의 결론을 서술한다.

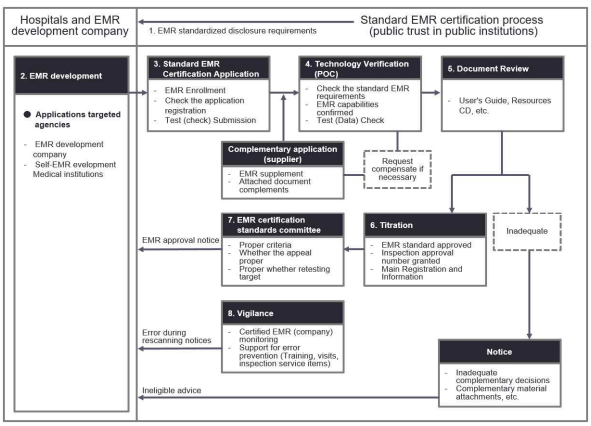

Fig. 1. EMR system approved standard system model

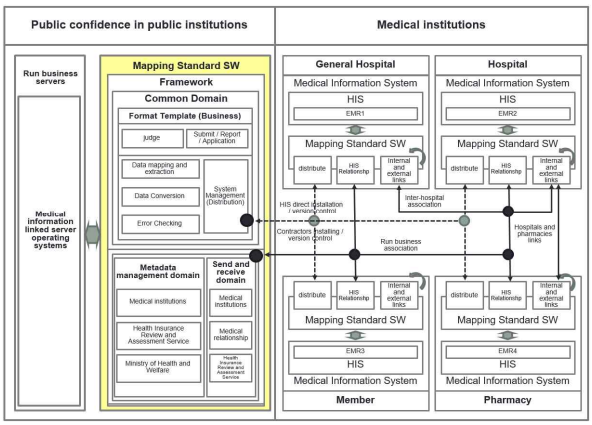

Fig. 2. Health care information exchange model mapped in accordance with the standards SW development spread

II. Real-time biometric data

생체 데이터(BIometric Data; BID)는 일상생활에서 쉽게 수집할 수 있는 맥박과 혈압(수축기와 이완기), 체질량 지수(Body Mass Index; BMI), 노화의 정도(Time Stamp; TS) 등을 대상으로 선정할 수 있다. 최근에는 심장 박동 수와 혈압 등을 간단하게 스마트 기기를 사용하여 측정 할 수 있는 앱들이 U-헬스의 기능을 담아 선보이고 있다. 이러한 여건을 배경으로 본 논문에서는 생체 데이터의 수집에 있어서 사람이 직접적으로 기계를 이용하여 측정하는 기존의 방식보다 무선 통신망을 통해 전송되는 사물인터넷 서비스 환경에서 측정되는 과정으로 전개한다. 생체 데이터의 수집범주는 능동적으로 지정할 수 있고 제한된 시간에 많은 양의 생체 데이터를 수집할 수 있다. 사물인터넷 환경에서 수집하는 과정[6]을 Fig. 3과 같이 나타냈다.

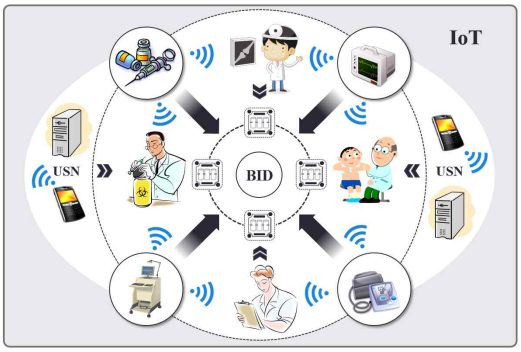

Fig. 3. IoT is collected in real-time on environment Biometric data

III. Security threats in biometric data

실시간으로 수집되는 생체 데이터에 대한 사용자 인터페이스와 수집된 생체 데이터를 패턴분석을 수행하는 과정[6]을 Fig. 4와 같이 나타냈다.

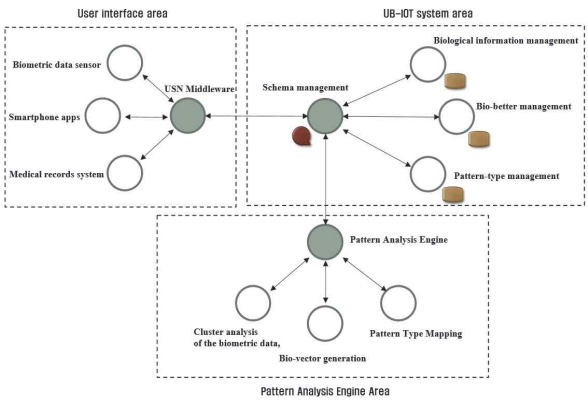

Fig. 4. Frame for processing the biometric data collected

Fig. 3에서와 같이 사물인터넷 환경에서 생체 데이터가 전송될 때 발생할 수 있는 보안 위협요인들을 크게 3개의 영역으로 구분하여 본 논문을 전개한다. 그리고 Fig. 4와 같이 보안 위협요소에 대한 요인을 파악하기 위해 사용자 인터페이스, UB-IOT 시스템, 패턴분석 엔진, 3개의 영역으로 구분하였다. 각 영역에서 생체 데이터의 보안을 위협하는 주요 요인을 살펴보면 다음과 같다.

1. User interface area

사물인터넷은 서버와 단말기에 대한 불법 접근과 정보의 조작, 탈취를 통한 기밀성/무결성 공격과 가용성 침해 등이 가장 취약한 부분이라고 할 수 있다. 이 영역은 생체 데이터를 실시간으로 수집하는 과정이므로 3개의 영역 중에서 보안이 가장 취약하다. 생체 데이터의 보안을 위협할 수 있는 요인으로는 비 인가된 접근, 정보유출, 데이터의 위조와 변조 등이 가장 취약한 위협 요인으로 분석된다.

2. UB-IOT system area

이 영역은 생체데이터를 수집하여 패턴을 분석하는 기존 연구[9]를 고찰하여 주요 보안 위협 요인을 분석하였다. 이 영역은 실시간으로 수집된 생체데이터를 데이터베이스에 저장하여 관리하는 영역으로 비 인가된 접근과 정보 유출 및 데이터의 위조와 변조 등이 취약하며 물리적인 장치 오류 등도 위협 요인으로 포함시킬 수 있다.

3. Pattern analysis engine area

생체데이터를 UB-IOT 영역에서 전달받아 군집분석과 바이오벡터의 생성, 패턴타입을 맵핑하여 UB-IOT 영역으로 전달하는 역할을 수행하는 영역이다. 이 영역에서는 생체 데이터에 대한 패턴분석을 수행하는 과정에서의 데이터 위·변조와 비인가자로부터의 접근 등의 보안을 위협하는 요인들이 존재한다.

IV. Security technology required by the IoT environment

사물인터넷 서비스는 유선과 무선으로 센서들을 전송해 준다. 사물인터넷 환경에서 노출된 보안 위협에 대응하기 위한 보안 요구 사항과 보안 기술[1][7-10]들에 대해서 고찰한다. 본 논문에서는 무선으로 생체 데이터를 전송할 수 있는 통신기술 중에서 RFID(Radio Frequency IDentification), 와이파이(Wi-Fi), 지그비(ZigBee) 보안기술과 사물인터넷 서비스 분야에서의 보안기술에 대해서만 다루기로 한다.

1. Security technology in RDIF environment

RFID는 비접촉식으로 사물에 부착된 태그 정보를 인식하는 무선 네트워크 기술이며 USN(Ubiquitous Sensor Network) 환경 구축에서 가장 비중을 많이 차지하는 기술이다.

RFID/USN 환경에서 사용되는 센서 네트워크의 특성을 고려할 때 안전한 플랫폼 설계가 요구되며 정보유출 등의 취약한 데이터의 보안을 위해 노드 간의 상호 인증을 위한 다양한 기법[9][11]들이 연구되고 있다.

2. Security technology in the Wi-Fi environment

Wi-Fi는 IEEE 802.11 표준을 기반으로 한 무선 랜 기술로 고성능 무선 통신이 가능하기 때문에 보안 위험으로부터 노출될 위협요인이 다른 환경에서보다 더 많이 존재한다. 무선 통신으로 송·수신되는 과정에서 암호화된 정보를 사용하지 않을 경우 비인가 접근과 도청, 스니핑 등의 공격을 받을 수 있는 취약성을 보유하고 있다. 무선통신 과정에서의 취약한 보안을 위해 암호화 알고리즘 CCMP(Counter mode with CBC-MAC Protocol)과 TKIP(Temporal Key Integrity Portocol)을 Wi-Fi 환경에서의 데이터 보안기술로 권장하고 있다[8].

3. Security technology in ZigBee environment

ZigBee는 유비쿼터스 컴퓨팅을 위한 통신기술로 IEEE 802.15.4 표준 중의 하나이다. 사무실이나 가정에서 무선 근거리 통신망을 사용할 수 있으며 저전력으로 전력소모는 적다. 하지만, 통신할 수 있는 정보량이 제한적이어서 높은 수준의 보안 기술을 적용하기 어렵다. ZigBee 통신망에서 사용할 수 있는 보안 기술로는 SSM(Standard Security Mode)과 HSM(Heig Security Mode)의 두 가지 방식이 존재한다.

적용기준은 보안 수준에 따라 낮은 수준의 SSM을 적용할 것인지 높은 수준의 HSM을 적용할 것인지를 요구하는 환경에 적용할 수 있도록 설계되었다. ZigBee의 각 장치는 Open Trust Model 방식으로 암호화되어 장치 내부의 신뢰성은 보장되지만, 외부와의 무선통신 환경에서의 보안 위협은 안전하다고 볼 수 없기 때문에 별도의 보안대책을 강구해야 한다[12].

4. IoT technologies in the security services sector

사물인터넷 응용서비스에서의 보안 요구사항은 크게 인증관리와 자원관리로 구분할 수 있다. 먼저, 인증관리는 사물인터넷 단말 미들웨어의 가상화 기술을 통해 외부로부터 유입되는 데이터로 인한 단말의 운영체제, 하드웨어 등이 영향을 받지 않도록 운영체제와 논리적 격리가 이루어져야 함을 의미한다[8].

사물인터넷 환경에서 전송받은 데이터는 비인가자가 아닌 인가자로부터 정당성을 인증 받은 단말기와 이를 통해 센싱되는 데이터가 정당성을 가지는 지에 대한 여부를 식별할 수 있어야 하고 전송되는 데이터의 정당성을 보장하기 위해 암호화

를 통한 무결성이 보장되어야 한다[9]. 이와 같이 사물인터넷 환경에서 보안 위협에 대응하기 위한 보안기술을 살펴보았다.

Ⅴ. Real-time biometric data security strategy

본 장에서는 4장에서 살펴본 사물인터넷 서비스 환경에서 생체 데이터가 실시간으로 전송되는 과정에서의 보안 위협 요인과 그에 따른 보안요구사항을 기반으로 생체 데이터의 안정성 확보를 위한 보안전략을 제안한다. 이와 관련하여 사물인터넷 서비스 환경에서 생체 데이터의 패턴분석을 위해 실시간으로 전송되는 생체 데이터를 수집하여 처리[6]하는 USN 미들웨어 디바이스를 Fig. 5와 같이 나타냈다.

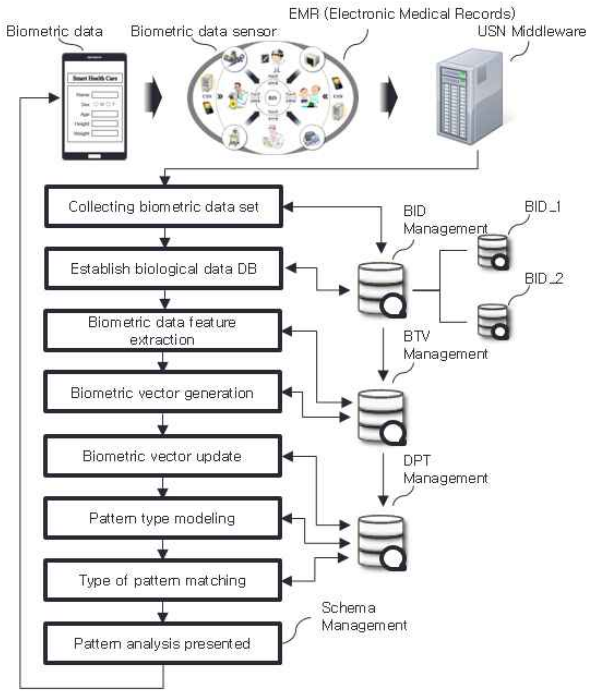

Fig. 5. USN middleware device

1. IoT Device security techniques applied

생체 데이터를 전송하는 사물인터넷 서비스 환경에서 사용되는 단말기와 센서들은 실시간으로 데이터를 전송하고 센싱하게 된다. 센싱과정에서 공급되는 전력은 제한적이며 처리능력 또한 한계적이다. 이러한 단점을 보완하기 위한 디바이스의 경량화와 저전력 암호화 기법이 필요하다. 특히, 기기 위변조 방지용 보안 SoC(System on Chip)와 보안 운영체제의 구축이 요구된다. 이와 관련하여 많은 연구들이 진행되고 있지만, 생체 데이터를 사물인터넷 서비스 환경에서 보안 위협으로부터 안전하게 전송하기 위한 디바이스의 암호화 기법이 지속적으로 개발되어야 한다.

2. IoT Object network security techniques applied

사물인터넷 환경은 매쉬형 토플로지의 형태로 구성되어 무선망을 통한 실시간 데이터를 전송하므로 보안이 구축된 게이트웨이와 침입탐지 및 대응기술이 필요하다. 또한 원격 보안관리와 관제기술을 통하여 실시간으로 모니터링 하여 사물 네트워크 환경에서 안전하게 데이터가 전송될 수 있도록 차별화된 보안 기법이 구축되어야 한다.

3. IoT Platform / services security techniques applied

사물인터넷 서비스 환경에서 생체 데이터를 효율적으로 전송하기 위해서는 사람 또는 사물에 대한 별도의 플랫폼과 식별자 통합관리가 필요하다. 현재의 서비스 형태가 향후 스마트폰 이외의 다양한 스마트 디바이스에 최적화되기 위해 사용자 인증기술 또한 다양하게 변화될 가능성이 있다. 따라서 개인프라이버시를 보호하고 유사시 익명성을 제거하여 신원확인이 가능하도록 스마트인증기술이 요구되며 생체 데이터를 보호하기 위한 통합적인 보안 솔루션이 개발되어야 한다.

본 논문에서 제안한 실시간 생체 데이터의 보안전략은 사물인터넷 서비스 환경에서 실시간으로 전송되는 생체 데이터를 안전하게 보호하기 위한 전략이다. 생체 데이터는 개인 프라이버시에 대한 민감한 데이터이므로 노출된 위협 요인들로부터 안전하게 보호되어야 한다. 이와 관련하여 본 논문에서 제안한 보안전략의 실효성을 제시하기 위해 USN 미들웨어 디바이스 보안과 사물 네트워크 보안, 플랫폼/서비스 보안기법을 적용하였을 경우의 기대효과에 대해 기술한다.

먼저, USN 미들웨어 디바이스에서의 보안기법은 병·의원에서 사용되는 종이 문서를 없애고 모든 데이터를 전산매체에 저장하는 전자의무기록시스템(EMR) 방식에 적용되어 확산되는 현 시점에서 반드시 필요한 보안기법이다. EMR은 의료사고가 증가함에 따라 의무기록의 법적인 가치증가로 임상적인 치료의 내용이 체계적으로 관리되어야하기 때문에 효율적인 데이터의 관리가 필요하다. 이러한 측면에서 생체 데이터는 각종 만성질환에 대해 예측할 수 있는 건강지표로 활용되기 때문에 디바이스에 대한 보안기법은 매우 중요하다. 디바이스 보안기법은 생체 데이터를 기기 위조와 변조 방지용 보안 SoC와 보안 운영체제를 구축할 경우 생체 데이터를 암호화하여 관리할 수 있다. 이와 같은 장점은 생체 데이터를 보안 위협요인으로부터 보다 안전하게 관리할 수 있다.

사물 네트워크 보안기법은 생체 데이터가 원격으로 전송되어 관리되기 때문에 실시간으로 모니터링 될 수 있도록 관제기술과 원격 보안관리가 철저하게 수행되어야 한다. 그렇기 때문에 기존 네트워크망의 보안기법에서 보안에 대한 기술이 업그레이드된 게이트와 침입탐지 및 대응기술로 위조와 변조, 인가되지 않은 접근, 도청, 스니핑 등의 위협 요인으로부터

생체 데이터를 보호할 수 있는 제반여건을 구축할 수 있다.

플랫폼/서비스 보안기법은 사람과 사물에 대한 플랫폼과 식별자를 통합 관리하여 생체 데이터를 효율적으로 전송할 수 있는 환경을 설정할 수 있다. 그렇기 때문에 생체 데이터에 대한 보안 위협요소를 미연에 방지할 수 있고 실시간으로 위협요인을 감시할 수 있다. 이 기법은 사전 탐지와 예방을 동시에 수행 할 수 있으므로 생체 데이터에 대한 실시간 감시와 통제가 가능하다.

이와 같이 사물인터넷 환경에서 실시간으로 전송되는 생체 데이터가 유출, 위조, 변조, 서비스 거부로부터 발생될 수 있는 보안취약 요인들을 사전에 예방하고 보안 위협요인들로부터 안전하게 생체 데이터를 보호하기 위한 보안전략을 디바이스 보안기법과 사물 네트워크 보안기법, 플랫폼/서비스 보안기법의 3가지 측면에서 접근하였다. 본 논문에서 제안한 보안전략을 구축할 경우 사물인터넷 환경에서 실시간으로 생체 데이터를 실시간으로 모니터링하고 통합 관리함으로써 기존의 생체 데이터 관리와 보안에 대한 위험요인 제거기술을 보완할 수 있으며 보안 위협요인들로부터 생체 데이터를 안전하게 관리할 수 있는 보안기술의 효율성을 높일 수 있다.

Ⅵ. Conclusion

최첨단 ICT 기술과 의료기술이 발달되어 ICT와 BT가 융합되는 바이오인포매틱스(Bioinformatics)라는 신조어가 탄생하게 되었다. 바이오인포맥틱스란 컴퓨터와 분석 소프트웨어를 활용해 생물학적 데이터를 얻고 이를 분석하여 생물학적 문제에 대한 답을 구하는 응용과학의 한 분야이다.

이와 같은 융·복합 기술로 인간의 수명은 계속해서 늘어나고 있으며 모든 사람들이 건강한 생활에 대한 관심도가 점차 높아가고 있다. 최근에는 사물인터넷 환경에서의 건강관련 정보들이 홍수처럼 쏟아지고 있으며 이를 기반으로 개인들도 본인의 건강한 정보와 상식에 대한 노하우를 가지게 되었다. 이와 관련하여 사물인터넷 환경에서 전송되는 실시간 생체 데이터의 특성상 데이터의 유출과 위조 및 변조, 서비스의 거부와 프라이버시 침해 등의 보안을 위협하는 요인들이 존재한다. 특히, 생체 데이터는 개인 프라이버시를 위한 가장 중요한 정보이므로 사물인터넷 서비스 환경에서 구성요소별 심각성과 우선순위를 고려한 보안 대책이 요구된다. 그리고 디바이스 보안기법과 사물 네트워크 보안기법, 플랫폼/서비스 보안기법에 대한 체계적이고 통합적인 관리시스템이 필요하다. 또한, 개인 프라이버시 보호를 위해 생체 데이터를 보다 안전하게 관리하기 위해서는 사물인터넷 서비스 내·외부적인 측면에서 발생할 수 있는 문제점에 대한 적극적인 대응책 마련이 시급하다.

따라서 본 논문에서는 실시간으로 전송되는 생체 데이터를 3가지의 영역으로 구분하여 보안에 취약한 위협요인과 요구되는 보안기술에 대하여 살펴보고 생체 데이터의 실시간 전송에 따른 안정성 확보를 위한 보안전략을 제안하였다. 본 논문에서 제안한 보안기법을 적용할 경우 사물인터넷 환경에서 실시간으로 전송되는 생체 데이터가 유출, 위조, 변조, 서비스 거부로부터 발생될 수 있는 보안취약 요인들을 사전에 예방할 수 있을 뿐만 아니라 실시간으로 모니터링 하여 통합관리 할 수 있는 기대효과를 제시하였다. 향후 사물인터넷 서비스는 전 산업분야에 빠르게 확산되고 있으므로 보안을 위협하는 요소들로부터 안전한 환경구축을 위하여 신규 보안기법에 대한 연구와 표준화 제정을 위한 추가적인 연구가 필요하다.

REFERENCE

[1] Bong-Im Jang, Chang-Su Kim, “A Study on the Security Technology for the Internet of Things”, Journal of Security Engineering, Vol.11, No.5, pp.429-438, August 2014.

[2] ITU-T Y.2060, Overview of the Internet of Things, 2012.

[3] Hye-Nam Kim, Yong Pa가, “Design of Context-Aware Middleware in Ubiquitous Computing Environment”, Korea society of computer and information Vol.10, No.5, pp.115-122, November 2005.

[4] Lee, Ki-Young ; Kim, Dong-Oh, “Design of a Location Management System in the Ubiquitous Computing Environments”, Journal of the Korea society of computer and information, Vol.12, No.6, pp.115-121, December 2007.

[5] http://www.bosa.co.kr/umap/sub.asp?news_pk=*598466*

[6] Yoon Hwan Shin, “Pattern Analysis of Biometric Data for the Needle Points Selection in Big Data Environments”, PhD thesis, Chungbuk National University, August 2014.

[7] A. Wrigh(2009), Cyter security for the power grid: cyber security issues & Securing control system, ACM CCS, Nov.9-13; Chicago, IL, USA.

[8] Donghee Kim, Seokung Yoon, Yongpil Lee, “Security for the IoT Service”, The Korean Institute of Communication and Information Sciences, Vol.30, No.8, pp.53-59, August 2013.

[9] Hae-soon Ahn, Eun-jun Yoon, Ki-dong Bu, In-gil Nam, “Secure and Efficient DB Security and Authentication Scheme for RFID System”, journal of

korean institute of communications and information sciences, Vol.36, No.4, pp.197-206, April 2011.

[10] Howon Kim, “Security issues in the IoT Serives”, Communications of the Korean Insitute of Information Scientists and Engineers, Vol.32, No.6, pp.37-41, June 2014.

[11] Jong-yeop Sung, Sang-duck Lee, Chang-ju Ryu, Seung-jo Han, “Mutual Authentication Protocol using One Time Password for Mobile RFID System”, Journal of the Korea Institute of Information and Communication Engineering, Vol.18, No.7, pp.1634-1642, July 2014.

[12] Bong-Hwan Kim, Jung-Mi Lim, Chang-Seop Park, “Analysis of ZigBee Security Mechanism”, Journal of Security Engineering, Vol.9, No.5, pp.417-430, October 2012.

Authors

Yoon Hwan Shin received the B.S., M.S. degrees in Computer Science and from Korea National University of Transportation and Ph.D. degrees in Computer Science and from Chungbuk University, Korea, in 1997, 1999 and 2014, respectively. Dr. Shin joined the Evaluation Committee of the KIAT(Korea Institute for Advancement of Technology) of Subcommittee member, Seoul, Korea, in 2014.

He is currently a Subcommittee member in the KIAT. He is interested in Database, Artificial Intelligence, Pattern Recognition, Big Data Processing and Security, Data Mining, IoT, USN Middleware, Ubiquitous and Mobile Computing, Biomedical and Bio-informatics.