ECG와 비콘 기반의 블록체인을 이용한 신원 인증 및 이상징후 탐지 기법

김경희[1], 이근호[2*]
[1]백석대학교 컴퓨터공학부 학생, [2]백석대학교 컴퓨터공학부 교수

A Scheme of Identity Authentication and Anomaly Detection using ECG and Beacon-based Blockchain

Kyung-Hee Kim[1], Keun-Ho Lee[2*]
[1]Student, Dept. of ICT, BaekSeok University
[2]Professor, Dept. of ICT, BaekSeok University

요 약 최근 생체 인증 기술이 발전함에 따라 생체 인증을 이용한 사용자 인증 기법들이 많아지고 있다. 기존에 존재하는 ID/PW 등 다양한 인증 기법에는 다양한 문제점이 제시되고 있다. 따라서 최근에는 2차 인증을 도입하여 보안성을 높이는 방식을 채택하여 사용하고 있다. 본 논문에서는 근거리 무선 장치(Beacon)와 다양한 생체 인증방식 중 심장의 전기적 생체신호를 이용하여 위·변조가 매우 어려운 특징을 가진 ECG를 이용하여 사용자의 신원 인증과 이상징후를 탐지할 수 있는 사용자 인증 시스템을 제안하고자 한다. 이 시스템은 손목에 장착 가능한 웨어러블 디바이스 형태의 ECG 측정 도구를 통해 기록한 ECG 데이터와 데이터베이스에 블록체인 형태로 저장된 신원 정보 및 생체데이터를 비교하여 일차적으로 신원을 확인하고 비콘(Beacon)을 활용하여 사용자의 위치를 파악함으로써 사용자의 이상징후를 탐지하고자 한다.

주제어 : 블록체인, ECG, 생체 인증, Beacon, 이상징후 탐지

Abstract With the recent development of biometric authentication technology, the user authentication techniques using biometric authentication are increasing. Various problems arised in certification techniques that use various existing methods such as ID/PW. Therefore, recently, a method of improving security by introducing biometric authentication as secondary authentication has been used. In this thesis, proposal of the user authentication system that can detect user identification and anomalies using ECGs that are extremely difficult to falsify through the electrical biometric signals from the heart among various biometric authentication devices is studied. The system detects user anomalies by comparing ECG data received from a wrist-mounted wearable device-type ECG measurement tool with identification and ECG data stored in blockchain form on the database and identifying the user's location through a beacon system.

Key Words : Blockchain, ECG, Identification certificate, Beacon, Anomaly detection

이 논문은 2020년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2020R1I1A3069008)
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2021년 7월 10일 수정일 2021년 8월 27일 심사완료일 2021년 8월 29일

1. 서론

최근 신원 인증의 수단으로 생체데이터를 이용한 신원 인증 시스템이 많아지고 있다. 기존에 널리 사용되던 ID/PW 방식의 경우 ID와 PW만 알고 있다면 본인이 아닌 다른 사람이 접근 할 수 있는 문제점이 제기되었고, 문제점의 해결 방안으로 생체 인증이 도입되었다.

생체 인증 기술이 발전함에 따라 기존 생체 인증방식에도 문제점이 제기되었다. 기존 생체 인증방식에는 홍채 인식, 지문 인식, 얼굴 인식 등이 있으며 생체데이터를 데이터베이스에 저장하여 대조하는 방식으로 사용되고 있다. 생체데이터는 개인만이 가지고 있는 고유한 특성으로 인증이 된다는 점에서 높은 보안성을 지니고 있다. 하지만 생체데이터의 원본이 유출되었을 경우 발생하는 문제점이 상당하다.

이에 본 논문에서는 “비콘과 ECG를 이용한 신원 인증 및 이상징후 탐지 시스템”을 제안한다. 본 시스템은 사용자가 ECG 측정이 가능한 웨어러블 장치를 손목에 부착하고 스마트폰을 소지한 상태로 비콘이 인식 가능한 반경에 접근하면 손목에 부착된 웨어러블 디바이스를 통해 ECG 데이터를 전송받아 생체정보를 이용하여 인증을 수행하고 신원을 확인한다. 또한, 비콘을 이용하여 사용자의 위치를 파악하여 접근할 수 없는 장소나 보안 등급이 정해진 장소에 접근하는 이상징후를 탐지하여 사용자와 관리자에게 이상징후를 알리고 위치와 간단한 신원 정보를 제공한다.

본 논문에서 제안한 시스템을 통해 연구실, 치매 병동, 회사 등 신원을 확인하고 이상징후를 탐지해야 하는 기관과 시설에 도입하여 빠르게 사용자의 신원 정보 및 위치를 파악하고 이상징후를 탐지하는 시스템을 제안하고자 한다.

2. 관련 연구

2.1 생체 인증

생체 인증 기술이란 인간의 지문, 얼굴, 정맥 음성인식 등 인간의 생리학 특징 및 행동특성 특성을 기반으로 개인이 지니는 독특한 특징을 본인 확인을 위한 측정 단위로 활용하는 기술로, 인간의 생체적인 특징을 자동화된 장치를 거쳐 신원확인에 이용하는 기술이다[1].

생체 인증방식은 본인이 지닌 생체적 특징을 이용하기 때문에 기존에 사용하던 ID/PW 방식처럼 아이디 및 패스워드를 기억할 필요 없고, ID/PW가 유출되었을 경우 누구나 접속할 수 있지만, 생체 인증의 경우 제3자가 로그인할 수 없다는 장점 때문에 신원 인증의 수단으로 널리 사용되고 있다.

생체 인증의 기술에는 홍채, 지문, 얼굴, ECG, 정맥, 음성인식 등 다양한 기술이 존재한다[2]. 생체 인증의 기술이 진화함에 따라 문제점 또한 지적되고 있다. 얼굴 인식의 경우 변장, 세월의 흐름, 성형수술 등으로 인한 인증실패 및 사진위조를 통한 보안의 문제점이 존재하며, 지문 인식의 경우 지문등록이 쉽고 높은 정확도를 가지고 있다는 장점이 존재하지만, 지문 유실에 의한 인증실패 및 지문 도난 등 문제점이 지적되고 있다[3]. 본 논문에서는 심장의 근육이 수축하면서 발생하는 전기적 신호를 활용한 ECG 인증방식을 사용할 것이다.

2.2 ECG

심전도는 심장의 근육이 수축하면서 발생하는 전기신호를 기록하는 것으로, 주로 병원에서 심장의 상태 및 질환을 진단하는 데 활용되고 있다. 최근에는 IOT 기술의 발전으로 웨어러블 디바이스 형태로서 심전도를 측정할 수 있는 제품들도 많이 나오고 있다. ECG는 개인별로 고유한 특징점을 가지고 있어 ECG를 이용한 인증이 가능하다. 또한, 심장에서 근육이 수축하면서 만들어지는 전기적 신호이기 때문에 위 변조가 어렵다는 장점이 있다[4].

ECG 인증방식의 경우 측정한 ECG를 대조하여 인증하는 방식의 경우 ECG 데이터의 원본을 데이터베이스에 저장하여야 하므로 유출의 위험이 존재하여 PQRST 특징점을 추출하여 특징점을 대조하는 방식을 이용할 것이다.

심전도 신호는 P파, QRS 복합파, T파로 구성되어 있다[5]. 심전도 신호 중 한 사이클의 데이터에서 가장 큰 값은 R값이 되고 이를 기준으로 특정 간격 사이에 들어오는 이전의 값이 Q값, 이후의 값이 S값이 된다[6].

본 시스템에서 제시한 ECG 인증은 대리 인증 및 스푸핑 공격 방지를 위해 사용하였다. 지문, 얼굴 인식, 홍채 인식의 경우 사용자가 스캐너에 인증 절차를 수행해야 하지만 ECG 인증의 경우 사용자가 ECG 측정이 가능한 웨어러블 디바이스만 장착하고 있다면 별도의 인증 절차 없이 인증이 된다는 장점 때문에 본 시스템에 적용하게 되었다.

2.3 비콘 (Beacon)

비콘은 블루투스 4.0 BLE(Bluetooth Low Energy) 프로토콜 기반의 근거리 무선통신장치이다[7]. 그중 블루투스 4.0의 버전부터 소비전력이 급격하게 감소하여 적은 용량의 배터리로도 1년 이상을 구동할 수 있어 블루투스4.0을 기반으로 한 BLE비콘이 주로 사용된다. 비콘의 인식 거리는 약 70M, 측위 오차 5cm 이내의 특성을 가지며, 전력 소모도 작아 특정 장소의 세부적인 위치 정보를 얻기에 최적화된 기술이다. 기존에 널리 사용되던 NFC 태그방식과는 달리 위치기반의 서비스를 제공하는 것이 가능하다. 비콘은 NFC와 같이 4~5cm로 근접할 필요도 없으며 GPS보다 정확한 위치 정보를 제공할 수 있기 때문에, 사용자의 위치정보를 추가적인 인증 요소로 활용할 수 있다[7-10]. 비콘은 기존 GPS기술로는 불가능하지만 신호의 세기를 조절하여 실내위치 정보를 파악할 수 있는 것이 GPS 기술과는 차별화된 큰 장점이다[11-12].

비콘은 별도의 연결 과정 없이 근거리에 블루투스만 활성화되어 있다면 스마트 기기를 자동으로 인식하여 통신할 수 있다. 비콘은 신호의 세기를 이용하여 위치를 파악하여 실내에서 GPS보다 정확한 위치를 제공하기 때문에 사용자의 위치 정보를 인증의 수단으로 사용할 수 있다. 또한, 비콘은 통신 반경 내에 있는 사용자는 비콘 메시지를 제한 없이 수신할 수 있으므로 암호화 과정을 거쳐야 한다.

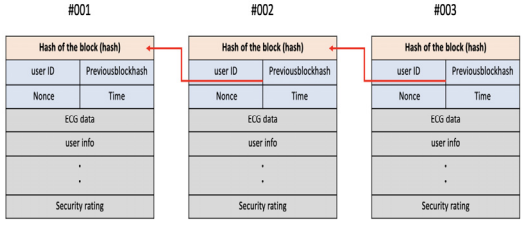
2.4 블록체인

블록체인은 데이터 처리 분산기술로서, 네트워크에 참여하는 모든 사용자가 모든 거래내역 등의 데이터를 분산, 저장하는 기술을 말한다. 블록체인은 체인 형태로 묶인 형태이기에 블록체인이라고 한다[13]. 기존의 중앙 집중형 클라우드 컴퓨팅 기술은 서버 – 클라이언트 – 서버 형태로 모든 정보가 한 곳에 집중되는 성격을 가졌지만, 블록체인은 이러한 중앙화 시스템에서 발생할 수 있는 문제를 해결하고자 제안된 방법으로 탈중앙화 형태의 분산 데이터 시스템이다. 블록체인에서는 일정 데이터를 디지털 서명한 후 p2p 네트워크로 연결된 노드들에게 전달하고, 전달된 데이터는 작업 증명의 방식으로 노드에 의해 승인되고, 승인된 데이터는 블록에 저장된다. 블록은 입력된 데이터의 해시값을 포함한다. 해시값을 통해 블록들은 서로 연결되어 있다. 어떠한 블록에서 변조가 일어나게 되면 이 블록에 저장된 해시값과 다음 블록에 저장된 해시값이 다르기 때문에 위 변조 여부를 빠르게 확인할 수 있다. 또한, 블록의 정보는 네트워크에 참여한 모든 노드들이 복제하여 가지고 있으므로 블록을 변조하더라도 다수의 노드를 통해서 변조 여부를 확인할 수 있다. 블록체인은 데이터의 무결성이 보장되고 모든 블록의 정보가 다른 참여자에게 복사되어 저장되기 때문에 투명성 또한 보장된다는 특징이 있다. 이러한 특징으로 생체데이터, 신원확인을 하는 용도에 적합하다[14-15].

3. 시스템 설계

3.1 DB 저장방식

본 논문에서 제안하는 시스템에서는 블록체인을 이용하여 블록체인 데이터베이스를 구축하고 이상징후 DB를 구축하여야 한다. 사용자의 개인정보, 보안등급, ECG 특징점 데이터를 암호화하여 관리함으로써 개인정보, 보안등급, ECG 데이터의 위조 및 변조를 방지하고자 한다. 개인정보, ECG 데이터 중 PQRST 고윳값을 식별 후 암호화하여 저장하는 이유는 블록체인의 특성상 모든 사람이 접근할 수 있기 때문에 개인정보는 암호화하여 저장하고 생체데이터의 경우 유출되면 복제가 가능할 수 있기 때문에 PQRST 고윳값을 식별하여 암호화하여 저장한다. 많은 DB구축방식 중 블록체인을 사용하는 이유는 데이터베이스에 저장된 생체데이터의 위조나 변조를 막기 위해 해시값을 통해 기밀성을 보장하는 블록체인 DB를 사용했다. 블록체인 내부 구조는 다음 Figure 1과 같다.



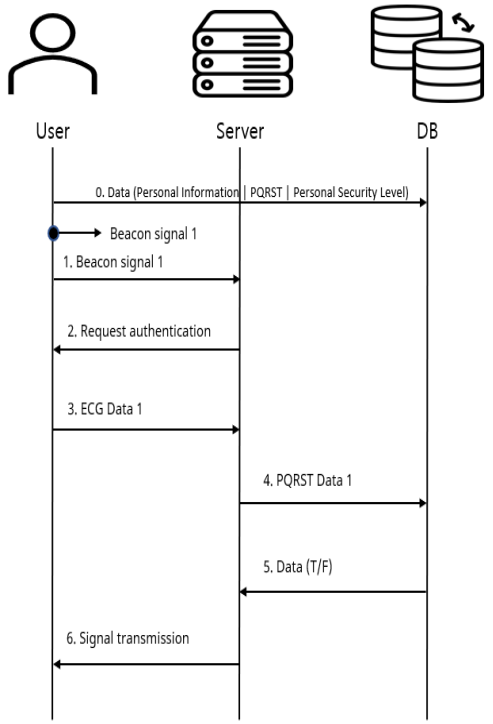
[Fig. 1] block chain Configuration diagram

3.2 이상징후 탐지

본 논문에서 제안된 시스템에서 이상징후를 탐지하는 방법은 다음과 같다. 본 논문에서 지칭하는 이상징후는 다음과 같다. 1. 일치하지 않는 ECG 데이터, 2. 부정인증, 3. 접근 불가한 위치로 구분한다. 사용자는 백그라운드로 실행된 애플리케이션에서 특정 주기마다 비콘신호를 수신한다.

3.2.1 일치하지 않는 ECG 데이터

사용자가 기관에 처음 출입 시 스마트폰에서 비콘 신호를 감지하여 애플리케이션을 실행한다. ECG 데이터 인증 절차를 통하여 블록체인 DB와 대조 절차를 거친다. 만약 등록되지 않거나 일치하지 않은 ECG 데이터를 감지할 경우 관리자에게 알림 문구를 띄워 호출한다. 정상적으로 인증 절차를 거친다면 신원 및 출입 시간을 데이터베이스에 저장하고 출입문을 연다. 절차는 아래의 Figure 2와 같다.



[Fig. 2] Unmatched ECG data

Step 0. 사용자의 개인정보, PQRST값, 개인 보안 등급을 암호화하여 DB에 저장한다.

Step 1. 사용자의 애플리케이션에서 비콘 신호를 감지하면, 서버로 비콘 감지 신호를 전달한다.

Step 2. 비콘 감지 신호를 전달받은 서버는 사용자에게 인증요청을 보낸다.

Step 3. 사용자의 웨어러블 기기를 통해 ECG를 측정하고, 서버로 전송한다.

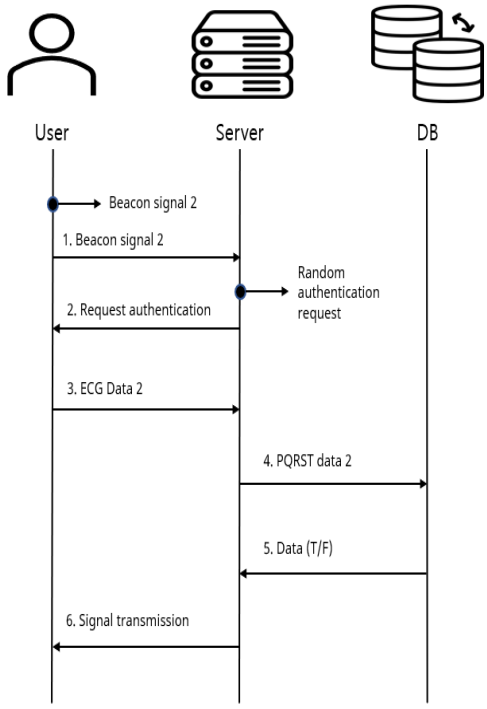
Step 4. 전달받은 ECG 신호의 PQRST 특징점을 추출하고 암호화되어 저장된 DB와 대조 절차를 거친다.

Step 5. DB와의 대조 절차를 거치고 성공 또는 실패 신호를 서버로 전송한다.

Step 6. 신호를 전달받은 서버는 사용자에게 성공 또는 실패 여부를 전달하고, 인증에 실패한 신호를 전달받았을 경우 사용자의 현재 위치 및 간단한 신원 정보를 관리자에게 전달 및 이상징후 DB에 저장 및 관리자를 호출한다.

3.2.2 부정인증

인증 절차를 거친 이후에 비인가자가 건물 내부에 존재하는 것을 방지하기 위해 시간을 무작위로 선정하여 사용자의 애플리케이션에 인증요청을 보낸다. 절차는 아래의 Figure 3과 같다.



[Fig. 3] Illegal verification.

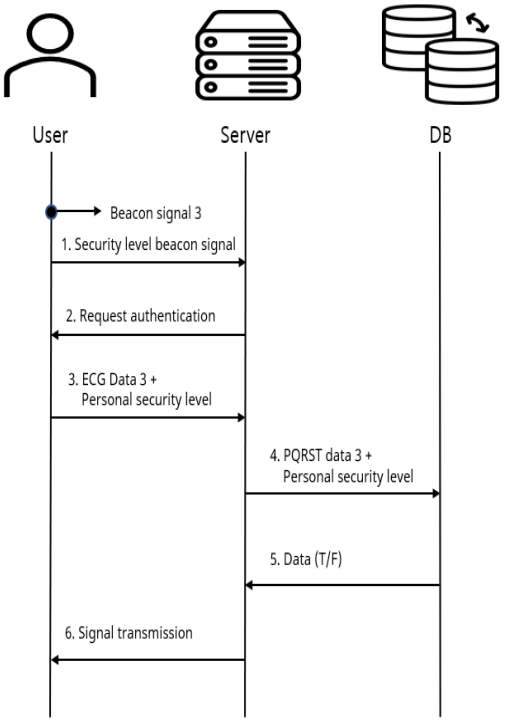
Step 1. 사용자의 애플리케이션에서 비콘 신호를 감지하면, 서버로 비콘 감지 신호를 전달한다.

Step 2. 비콘 감지 신호를 전달받은 서버는 무작위로 시간을 설정하여 사용자에게 인증요청을 보낸다.

Step 3. 사용자의 웨어러블 기기를 통해 ECG를 측정하고, 서버로 전송한다.
Step 4. 전달받은 ECG 신호의 PQRST 특징점을 추출하여 암호화되어 저장된 DB와 대조 절차를 거친다.
Step 5. DB와의 대조 절차를 거치고 성공 또는 실패 신호를 서버로 전송한다.
Step 6. 신호를 전달받은 서버는 사용자에게 성공 또는 실패 여부를 전달하고, 인증에 실패한 신호를 전달받았을 경우 사용자의 현재 위치 및 간단한 신원 정보를 관리자에게 전달 및 이상징후 DB에 저장 및 관리자를 호출한다.

3.2.3 위치 이상징후

접근할 수 없는 보안등급의 사용자가 접근하는 것을 막기 위해 최초 회원가입시에 관리자는 보안등급을 지정한다. 보안등급이 정해진 비콘 데이터를 수신받으면 애플리케이션을 실행하고 ECG 인증 절차를 거친다. 절차는 다음 Figure 4와 같다.



[Fig. 4] Location abnormality.

Step 1. 사용자의 애플리케이션에서 보안등급이 지정된 비콘 신호를 감지하면, 서버로 비콘 감지 신호를 전달한다.
Step 2. 비콘 감지 신호를 전달받은 서버는 사용자에게 인증요청을 보낸다.
Step 3. 사용자의 웨어러블 기기를 통해 ECG를 측정하고, 애플리케이션에 저장된 보안등급을 서버로 전송한다.
Step 4. 전달받은 ECG 신호의 PQRST 특징점을 추출하고 암호화된 PQRST 및 보안등급을 사용자가 전송한 데이터와 DB의 대조 절차를 거친다.
Step 5. DB와의 대조 절차를 거치고 접근 승인 및 실패 신호를 서버로 전송한다.
Step 6. 신호를 전달받은 서버는 사용자에게 접근 승인 및 실패 여부를 전달하고, 인증 및 접근 승인에 실패한 신호를 전달받았을 경우 사용자의 현재 위치 및 간단한 신원 정보를 관리자에게 전달 및 이상징후 DB에 저장 및 관리자를 호출한다.

4. 결론

본 논문에서는 ECG와 비콘을 이용한 사용자 신원확인 및 이상징후 탐지 시스템을 제안하였다. 본 논문에서 제안된 시스템이 도입되었을 때의 효과는 다음과 같다. 기존에 사용하던 지문 인식, 얼굴 인식, 홍채 인식의 문제점으로 지적되었던 지문 소실, 성형 등 생체데이터의 변화로 인한 인식의 문제를 해결할 수 있는 ECG를 도입하여 인식의 보안성을 향상했다. 개인이 가지는 심장의 전기적 신호인 ECG를 통해 인증 함으로써 사용자의 신원을 확인할 수 있다. 또한, 비콘을 사용하여 사용자의 위치에 대한 이상징후까지 탐지해 낼 수 있는 시스템을 제안하였다. 제안한 시스템은 별도의 조작 없이 ECG 측정이 가능한 웨어러블 디바이스만 장착하고 있으면 인증이 가능하므로 스마트폰 조작이 힘든 병원 등 다양한 시설에서 활용이 가능할 것으로 본다. 하지만 ECG의 특성상 과도한 움직임이 있을 시, 인증이 어렵다는 문제가 있어 심박수 측정 및 다양한 수치를 결합하여 인증의 정확성을 향상시켜 ECG 생체 인증의 단점을 보완하고 시스템의 구체적인 설계, 보안 요소를 추가하여 향후 프로토타입을 구현할 예정이다.

REFERENCES

[1] J.H Kim and K.s Park., “Personal authentication using bio-signals Technology and DB construction”, TTA Journal. Vol.165, 2016.

[2] H.W Yang, J.W Jang, J.H Park, Y.C Lee and D.Y Kim, "The electronic access list system based on beacon and biometric authentication technology." Collection of papers at the academic conference of the Korean Society of Communications. pp.927-928, 2021.

[3] J.C Choi, S.H Seo, D.H Yang, and K.H Lee, “Relay attack response in BLE intensive analysis”. Journal of the Korean Society for Next-Generation Computing. Vol11.4, pp.25—35, 2015

[4] J.h Lee, G.h Chae, G.y Lim, J.h Seol, S.m Choi and S.g Lim., “Attendance Check System combining Beacons and Biometrics”, THE JOURNAL OF KOREAN INSTITUTE OF NEXT GENERATION COMPUTING. pp.24—32, 2018.

[5] G.R Kim and D.H Lee. “Protection for Single Management and Utilization.”, pp.279-327, 2019

[6] S.J Im, H.D Kwon and H.J Seo, “Non-cooperative system, iris recognition, identification system of complex system.”, Journal of Information Processing Society. Commands and Systems. pp.1-6, 2021.

[7] J.W Heo, S.W Jin and J.S Jeon, “Implementation and Evaluation of Valid ECG Systems.” Journal of the Korean Society for Industry-Academic Technology. pp. 1—6, 2019.

[8] S.J Kang and S.K Lim , "Designing and implementing beacon-based electronic access lists for Pandemic response." pp.83-91, 2021.

[9] H.Y Kim, H.J Kim and S.S Shin. "Automated access management system using beacons." pp.105-107 2021.

[10] H.R Park, N.H Kim, S.G Kim, H.G Son ."Building a positioning system using signal strength of drones and BLE beacons." Academic Conference of the Korean Society of Spatial Information . pp.137-138, 2020.

[11] D.H Yoo, K.H Kim, S.H Kim, B.J Yoon and H.Y Yeom ."Trend of biometric authentication method using veins. pp.79-84, 2015.

[12] S.W Jin, S.S Kim and M.S Jun, "Suggestion of User Authentication System for Safe Vehicle Control With ECG Waveform", The KIPS Fall Conference 2018 on Korea Information Processing Society, Vol.25, No.2, pp.227-230, 2018.

[13] Y.M Ki, "Biometrics Technology Status and Prospects, Special Report", TTA Journal, No.98, 2015.

[14] D.M Choi. "Analyzing and Proposal of Smartphone Authentication Techniques Using Biometric Recognition." pp.875-885, 2018.

[15] H.J Moon, "Safe authentication technique based on biometric information and OTP using blockchain." Convergence information paper 8.3, pp.85-90, 2018.

김 경 희(Kyung-Hee Kim) [준회원]

■ 2020년 3월 ~ 현재 : 백석대학교

〈관심분야〉

디지털 포렌식, 모의 해킹, 개인정보보호

이 근 호(Keun-Ho Lee) [종신회원]

■ 2006년 8월 : 고려대학교 컴퓨터학과(이학박사)

■ 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원

■ 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수

〈관심분야〉

이동통신 보안, 융합보안, 개인정보보호, 블록체인