사물인터넷 환경에서 블록체인을 이용한 정보보호 기법

이근호*
백석대학교 ICT학부 교수

A Scheme for Information Protection using Blockchain in IoT Environment

Keun-Ho Lee*
Professor, Div. of Information Communication Technology, BaekSeok University

요 약 4차 산업혁명시대로 접어들면서 많은 기술들의 발전이 이루어지고 있으며 다양한 위협요소들이 생겨나고 있다. 이러한 위협요소에 대응하기 위한 연구가 많은 분야에서 이루어지고 있다. 다양한 분야의 발전중에서도 의료기술과 지능형 자동차의 발전으로 인한 위협요소는 의료에 대한 잘못된 정보로 인한 생명에 대한 위협과 지능형 자동차를 통한 사람의 안전한 운행을 방해하여 생명을 위협하는 요소들이 가장 큰 위협요소로 대두되고 있다. 본 논문에서는 환자의 정보가 중요한 만큼 환자의 의료 기록에 대한 안전성과 신뢰성이 있는 기술을 위하여 블록체인의 기술 종류 중 프라이빗 블록체인을 사용하여 환자의 의료 기록에 대한 안전성과 효율성, 확장성을 높이는 방법과 자동차 시스템을 해킹하여 운전자의 생명을 위협하고 개인정보 및 위차파악으로 사생활 문제점에 대한 해결과 사물인터넷에서의 위변조를 방지하기 위하여 블록체인 기술을 이용한 정보보호 기법을 제안한다.

주제어 : 사물인터넷, 의료정보, 지능형자동차, 블록체인, 위협

Abstract Entering the 4th industrial revolution, many technologies are developing and various threats are emerging. In order to cope with such threats, research is being conducted in many fields. Even in the development of various fields, the threats caused by the development of medical technology and intelligent vehicles are the threats to life due to misinformation about medical care and the threats to life by preventing the safe operation of people through intelligent vehicles. In this paper, as the patient's information is important, the private blockchain is used to increase the safety, efficiency, and scalability of the patient's medical records. We propose an information protection technique using blockchain technology to hack the car system and threaten the driver's life, solve privacy problems by identifying personal information and differences, and prevent forgery in the Internet of Things.

Key Words : Internet of Things, Medical Information, Intelligent Vehicles, Blockchain, Threats

1. 서론

사물인터넷 시대로 접어들면서 다양한 디바이스에서 발생할 수 있는 위협요소로 인하여 최근에는 개인 또는 사회를 위협하는 지능형 범죄들이 증가함에 따라 사회의 불안요인으로 인한 다양한 해결 방안에 대한 요구사항이 높아지고 있다. 이러한 새로운 4차 산업혁명시대로 접어들면서 많은 기술들의 발전이 이루어지면서 다양한 위협

본 논문은 2019년 백석대학교 학술연구에 의하여 지원되었음
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2019년 10월 11일 수정일 2019년 11월 25일 심사완료일 2019년 12월 12일

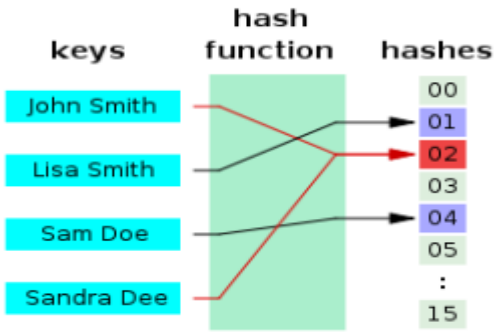
www.kci.go.kr

요소들이 생겨나므로서 위협요소를 방어하기 위한 연구가 많은 분야에서 이루어지고 있다. 다양한 분야의 발전 중에서도 의료기술과 지능형 자동차의 발전으로 인한 위협요소는 상당히 중요한 사회적 위협요소가 되고 있다. 기존의 위협요소는 개인 정보에 대한 탈취나 시스템에 대한 파괴나 서비스에 대한 거부등의 보안 이슈였다고 하면 현재의 4차 산업혁명시대의 정보보안 이슈는 수많은 디바이스의 연결로 인한 사람에 대한 안전이 큰 이슈로 대두되고 있다. 그중에서도 특히 의료에 대한 잘못된 정보로 인한 생명에 대한 위협과 지능형 자동차를 통한 사람의 안전한 운행을 방해하여 생명을 위협하는 요소들이 가장 큰 위협요소로 대두되고 있다. 본 논문에서는 환자의 정보가 중요한 만큼 환자의 의료 기록에 대한 안전성과 신뢰성이 있는 기술을 위하여 블록체인의 기술 종류 중 프라이빗 블록체인을 사용하여 환자의 의료 기록에 대한 안전성과 효율성, 확장성을 높이기 위한 블록체인을 이요한 정보보호기법과 지능형 자동차의 안전성을 위한 정보보호 기법을 제안하고자 한다. 논문의 구성은 관련연구에서 블록체인에 대한 기본 개념과 의료정보와 지능형 자동차의 ECU, 사물인터넷에서의 취약점에 대하여 살펴보고, 의료정보와 지능형 자동차 및 사물인터넷에서 적용가능한 블록체인을 기반으로 한 정보보호 기법을 제안한다.

2. 관련연구

2.1 블록체인

블록체인은 기존의 네트워크 방식이었던 P2P방식을 기반으로 데이터들이 해쉬암호화를 통한 체인형태의 연결고리 기반으로 분산 저장되어 있다. 블록체인은 기존의 중앙집중 방식인 데이터를 지속적으로 서비스 참여자들에게 모두 전송하고 데이터 내역을 중앙에서 관리하는 것이 아닌 각 이용자들이 보관하는 형태로 저장하는 탈중앙화 기술이다[1,2]. 블록체인은 변조를 판단하기 위하여 정보들을 모은 블록의 Fig 1의 방법으로 해쉬를 만드는데 해쉬를 만들 때마다 이전 블록의 해쉬값을 입력하여 현재 블록의 해쉬를 만들어 영향을 끼치게 한다. 블록체인은 중앙관리체제로 운영되는 클라우드와 비교되는 네트워크의 구조이고 분산형 구조 형태로 모든 데이터 정보를 가지고 있다. 또한 중앙 서버에 모든 정보를 처리하는 클라우드 방식과는 다른 네트워크 방식으로 동작한다. 블록체인은 데이터 정보를 하나에만 저장하지 않고 여러 곳으로 분산하여 분산된 형태로 배치되기 때문에 데이터가 변조될 가능성은 매주 낮으며 중앙서버에서 관리하는 형태가 아니기 때문에 사용자의 모든 데이터 정보를 가지고 있으며, 중앙체제에서는 서버에 저장한 정보를 보호하기 위하여 시스템들을 보안하여 운영한다. 그러므로 정보를 서버에 저장하는 방식 및 보안에 필요한 인력의 유지비용으로 소모하게 된다. 블록체인의 방식은 중앙관리체제가 필요하지 않은 방식이라서 중앙서버에서 소모되는 유지비용이 적게 든다[3-5].



[Fig. 1] hash function process(Source Wikipedia)

블록체인은 프라이빗 블록체인(private blockchain)과 퍼블릿 블록체인(public blockchain)으로 나뉜다. 프라이빗 블록체인은 채굴자의 역할이었던 기존의 퍼블릭 블록체인 시스템과는 다르게 거래 과정 검증을 블록의 승인권한을 가진 관리 주체가 직접 채굴하는 시스템이다[6]. 또한 블록에 대한 검증 주체가 채굴자가 아닌 중앙의 시스템 관리 주체로 이동하게 되면서 블록체인 시스템의 주 개발 목적인 탈중앙성과 개방성은 비교적 약하지만 프라이빗 블록체인은 기존의 블록체인 시스템과 비교했을 때 저장 정보의 다양성과 빠른 처리 성능을 제공한다. 그리고 기존 블록체인 시스템에서 필수적인 과정이었던 채굴 과정을 생략하기 때문에 블록이 만들어지는데 걸리는 시간은 기존의 블록체인보다 비교적 짧다[7]. 이는 블록체인의 처리 성능과 관련 있으며 프라이빗 블록체인은 허가 받은 소수의 사람들이 참여하기 때문에 열람하는 할 수 있는 사람들에게 열람 권한에 제한을 두어야 한다. 이는 열람 권한에 제한하는 정보를 저장하는 데에도 사용할 수 있다. 때론 필요에 따라 임의로 제한이 가능하다. 프라이빗 블록체인은 허가받은 사람들이 참여하기 때문에 기밀성이 강화될 수 있으며 신뢰할 수 있는 블록체인이다[8].

www.kci.go.kr

2.2 블록체인 적용 분야

블록체인 적용분야는 많은 분야가 있지만 이중에서 의료관련 분야, 지능형 자동차 관련 분야, 사물인터넷에 대한 정보보안 관련 분야를 다루고자 한다.

- 의료정보

의료정보는 우리나라 국민의 의료기관과 진료정보, 유관기간, 제약회사 등 여러 경로를 통해 수집한 정보를 분석하여 정제한 데이터이다. 그뿐만 아니라 환자들의 수술, 의약품, 의료기기 정보 등 의료 자원 데이터들을 모아둔 것을 말한다. 기본적으로 환자들의 개인 정보들을 많이 보관하고 있다. 이 때문에 정보에 대한 민감성으로 이 부분에 있어 많은 주의를 기울여야 한다. 1년에 지속적으로 발생하고 있는 의료사고를 보았을 때 한 생명을 다루는 만큼 환자의 의료 기록은 중요하고 민감하고 예민할 수 밖에 없다. 의료정보는 제일 중요하기 때문에 데이터의 높은 신뢰성이 있어야한다[8,9].

- 지능형 자동차

지능형 자동차는 ECU(Electronic Control Unit)를 통하여 전자제어 장치로 자동차의 모든 동작을 전자적으로 관리하며 자동차의 제어 하는 전자 장치로서 엔진, 변속기, 조향, 제동, 현가장치 등을 제어하는 장치로써 기존의 목적과는 다르게 점차 기술이 발전하면서 기능들이 많아져 ECU가 제어하는 기능들이 점차 많아지고 있다[10,11]. 또한 모든 동작을 제어하고 관리하는 역할을 하고 지능형 자동차에 중요한 역할을 하고 있으며 매우 중요한 장치이다. ECU는 크게 입력, 출력, 연산으로 구분할 수 있다. 입력은 출력값을 주로 보고 연산과 출력은 제어장치의 제어를 보고 있다[12].

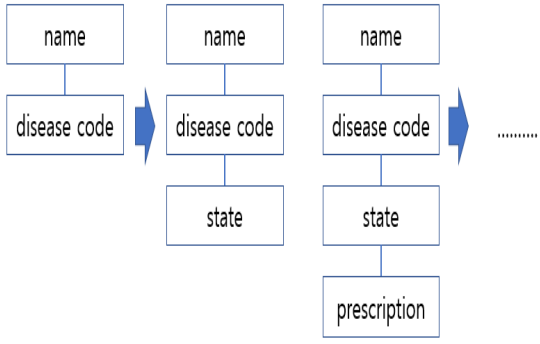
- 사물인터넷 위변조 취약점

정보를 저장 해야 하는 중앙서버의 서버 유지비, 보안 등부터 기존 IoT의 문제점은 생각보다 많다. 2016년 10월 21일, 미국에서 다인(Dyn) 회사가 DDos 공격을 당함에 아마존(Amazon), CNN, 페이팔(PayPal), 트위터(Twitter) 등의 85개의 웹 서비스가 중지되는 초유의 사태를 맞았다[13]. 이 공격은 단순한 좀비 PC를 이용한 DDos 공격이 아닌 IoT 기기들을 이용한 공격이라는 것을 눈여겨봐야 한다. 다인(Dyn)을 공격한 것은 바로 미라이(Mirai) 봇넷(Botnet)이었다. 다인을 공격하는 데 쓰인 IoT의 기기 수는 약 10만 개에 달하였고, 초당 1.2테라 바이트의 공격이 감행되었다고 다인 관계자는 말했다[14]. 이렇게 IoT 기기들이 무방비하게 놓여져 있는 이유 중 하나는 IoT의 특성상 작은 기기들이기 때문에 CPU 또한 그만큼 퍼포먼스가 낮을 수밖에 없다. 이러한 낮은 CPU의 퍼포먼스 때문에 공개키 암호화 방식을 사용할 수 없는 경우도 많고, CPU 자체에서 암호화 기능을 지원하지 않는 경우도 있다[13]. 또한, IoT 센서를 이용하여 명령을 내릴 때, 패킷이 암호화가 되어 있지 않을 경우 해커는 스니핑을 통하여 패킷의 내용을 알아내 어떠한 방식으로 명령을 내리는지 알 수 있다. 이를 이용하여 스마트 도어락이나 가스 밸브 등의 생명에 위험을 줄 수 있는 제어 행위를 해커는 마음대로 할 수 있을 것이다[15].

3. 블록체인 적용을 통한 정보보호 기법

3.1 의료정보 기반 블록체인 적용 기법

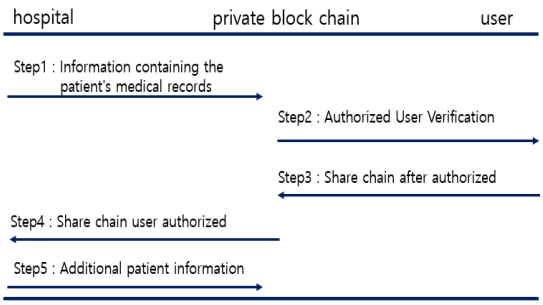
환자의 정보를 담고 있는 체인을 한 사람의 고유 ID를 발급하여 그 안에 정보를 저장한다. Fig 2는 병원에서 사용하고 있는 의료정보에 대한 것으로 환자의 상태, 병명 코드, 처방약 등 그 안에 환자의 의료 정보 데이터를 계속해서 연결한다. 환자의 정보가 지속적으로 업데이트가 될 경우에는 지속해서 체인을 연결한다.



[Fig. 2] chained medical information

Fig 3은 프라이빗 블록체인을 통한 진행과정에 대한 것이다. 의료 정보 가운데 환자의 민감한 정보가 많이 들어있다. 환자의 나이, 병명, 처방된 약 등 이러한 민감한 정보들이 많은 가운데 한 중앙에서 모든 권한을 가지며 허가 받은 사람들만 접근할 수 도록하는 프라이빗 블록체인을 사용하여 환자의 민감한 정보를 보호할 수 있도록 Fig 3과 같은 기법을 제안한다.

www.kci.go.kr



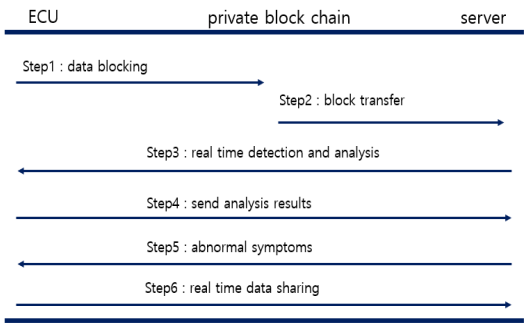
[Fig. 3] medical information system using private blockchain

Step1 : 병원은 검증이 완료된 중앙기관에 환자의 진료 기록이 담긴 정보를 전송한다.
Step2 : 인증기관은 사용자가 허가된 사용자임을 확인한다.
Step3 : 허가된 기관, 사용자인 경우, 그 연결된 체인을 공유하며 환자의 진료데이터를 볼 수 있다.
Step4 : 허가된 기관에서는 병원에 공유된 환자의 진료데이터에 대한 권한을 부여한다.
Step5 : 만약 환자에 대한 정보가 추가될 경우, 블록에 다시 연결한 후 전송하여 인증기관으로 보낸다.

이처럼 프라이빗 블록체인을 사용하면 허가받은 사람들만의 자료에 접근할 수 있으며 누구인지 식별이 가능하기 때문에 어떠한 사용자가 들어왔는지 등 확인할 수 있으며 기밀성을 유지할 수 있도록 의료정보 시스템의 정보보호 기법을 제안한다.

3.2 지능형 자동차 기반 블록체인 적용 기법

Fig 4는 지능형 자동차에서 ECU를 통한 프라이빗 블록체인에 적용하여 서버와의 연동에 대한 기법을 제안하여 안정성을 높이는 방법을 제안한다. 프라이빗 블록체인을 기반으로 하는 것은 특별한 안전성을 위하여 특수하게 프라이빗 기반의 블록체인의 구조를 통하여 지능형 자동차에서 발생되는 모든 정보를 제어할 수 있도록 하기 위한 과정으로 설계를 하고자 한다. 기존의 제어 시스템에서 블록체인의 기술을 적용하여 데이터를 블록화 하여 높은 보안성을 지니고 자율 주행자동차를 관리하는 서버에 한 개의 자동차가 해킹 공격이 들어오게 되면 모든 차에게 알리고 그 차에 대한 통신을 거부하고 1차 보안성을 유지하고 블록체인 기술을 적용하는 기법을 제안한다.



[Fig. 4] ECU application model using blockchain

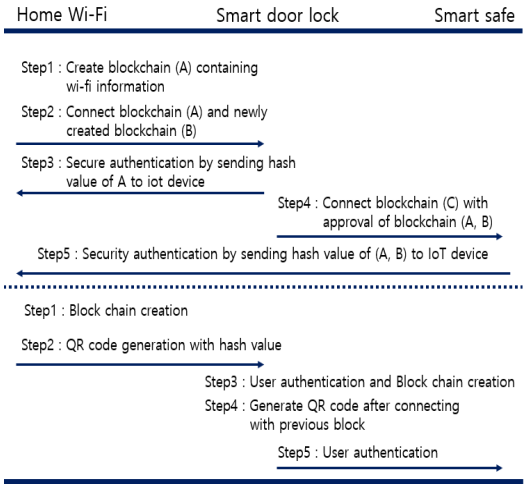
Step1 : 데이터 값을 전송하고 블록화한다.
Step2 : 전송받은 블록의 데이터를 서버에 저장하고 관리한다.
Step3 : 실시간으로 침입탐지 및 분석을 하고 나서 차량 점검을 시작한다.
Step4 : 분석이 끝나게 되면 서버로 값을 전송하고 받은 데이터 값을 저장하게 된다.
Step5 : 만약 이상징후 데이터가 탐지되면 즉시사용자에게 알림이 전송되고 로그가 남게 된다.
Step6 : 즉시 차량의 자율주행 시스템을 정지하고 수동으로 운전자에게 넘겨주고 점검을 받게 된다. 실시간으로 데이터를 공유하면서 사전 문제점을 차단한다.

3.3 블록체인을 이용한 스마트홈 위변조 방지 기법

IoT의 기기 특성상 사용자의 민감한 개인정보를 수집하고 요구하고 수집하는데, 이 정보들이 다른 사람들에게 노출이 될 경우, 심각한 사생활 피해 및 재산 손괴를 유발할 수 있다. 예를 들어, 스마트 홈(Smart Home)이 해킹될 경우, 카메라를 이용한 사용자의 사생활 침해와 스마트 카(Smart Car)가 해킹이 될 경우, 자율주행을 기능을 이용하여 인명 피해 및 재산 피해를 줄 수 있다. 이를 방지하기 위하여 프라이빗 블록체인을 이용한 디바이스 인증 기법을 제안한다. 이는 블록체인에 연결된 IoT 기기들은 서로의 정보를 블록체인에 담아 서로를 보증하기 때문에 위/변조를 막고 승인 없이 다른 IoT 기기들이 함부로 침입하지 못하게 하는 시스템을 구축하여 보안을 한층 강화 할 수 있다. 한단계 더나아가서 공격자가 IoT 기기들이 보내는 패킷을 스니핑 하여 어떠한 방식으로 명령을 전달하는지 알아내어 스마트 홈에 연결되어 있는 기기들을 해킹 할 수 있으므로, 비정상적인 패킷 또한 차단하는 기능 또한 추가된다.

www.kci.go.kr

Fig 5와 같이 IoT의 대표적인 스마트 홈을 기반으로 구성되어 있으며 모든 블록체인은 프라이빗 블록체인으로 서로 연결되어 있어 서로의 정보를 보호할 수 있고 패킷 정보 또한 안전하게 보낼 수 있을 것이다.



[Fig. 5] Smart home using blockchain

스마트홈에서의 블록체인 적용 기법의 효과는 두 가지의 효과를 불러올 수 있다.

첫 번째로, 홈 Wi-Fi에서 블록체인을 바탕으로 여러 IoT 기기들을 연결하는 것이다. 과정은 아래와 같다.

Step1 : 홈 Wi-Fi의 정보가 담긴 블록체인(A)을 생성시킨다.

Step2 : 스마트 도어락(Smart Door Lock)의 정보가 담긴 블록체인(B)을 생성 한다.

Step3 : 홈 Wi-Fi의 해쉬 값을 IoT 기기에 보내 인증을 보낸 후, 보안인증을 한다. 해쉬값이 맞을 경우, 두 기기를 연결 한다.

Step4,5 : 또 다른 IoT 기기인 스마트 금고(Smart Safe)를 연결할 경우에는 블록체인(C)을 생성 후, 기존의 블록체인(A, B)의 해쉬값을 받고 정보가 맞을 경우 세 개의 블록체인(A, B, C)을 연결한다.

두 번째로, 보통의 경우에는 사용자가 IoT 기기를 사용 등록을 할 때 기기와 동봉된 QR코드로 인증을 하지만, 블록체인을 사용할 경우, 해쉬값을 기본으로 한 QR코드로 인증을 하여, 공격자가 사용자의 애플리케이션을 해킹하여도 어떠한 기기를 사용하는지 알 수 없게 하는 기법을 제안한다.

Step1,2 : 홈 Wi-Fi의 정보가 담긴 블록체인(A)을 생성시킨다.

Step3,4,5 : 해쉬값을 이용하여 QR코드를 생성하고, 사용자 인증을 진행한다.

4. 제안 기법에 대한 안전성 분석

본 논문에서 제안하는 사물인터넷 기반에서의 블록체인 기반 정보보호 기법은 크게 의료정보, 지능형 자동차, 사물인터넷 홈네트워크에 대한 블록체인을 적용하는 기법을 제안하였다. 각 제안했던 정보보호기법은 사물인터넷에서 블록체인을 기반으로 하여 정보보안의 기본 요구사항인 안정성을 충족하고 있다.

- 의료정보관련 안전성

의료정보를 블록체인의 안전성을 좀더 고려한 프라이빗 블록체인으로 이용할 수 있는 기법을 제안하고, 의료데이터에 대한 사용은 허가받은 사람들만의 자료에 접근할 수 있도록 하여 기밀성을 보장하고, 블록체인으로 구성한 블록이 인증 이후에 누구인지 식별이 가능하기 때문에 어떠한 사용자가 들어왔는지 등 확인할 수 있는 가용성을 충족하고 있으며 블록체인화를 통한 데이터에 대한 무결성을 유지할 수 있어 정보보호의 3대 기본요소인 기밀성, 가용성, 무결성을 만족하고 있다.

- 지능형 자동차 관련 안전성

지능형 자동차에서 사용이 되고 있는 데이터 값을 전송시 블록체인화를 통하여 무결성을 보장하여 외부 해커로부터의 데이터 왜곡을 방지할 수 있는 기능을 제공 할 수 있다. 전송받은 블록의 데이터를 서버에 저장하고 관리하여 가용성을 높일 수 있다. 실시간으로 침입탐지 및 분석을 하고 나서 차량 점검을 시작하므로 기밀성과 무결성의 기능을 강화할 수 있다. 실시간으로 데이터를 공유하면서 사전 문제점을 차단하므로 사고를 미연에 방지할 수 있어 다양한 정보보호에 대한 기능을 충족한다.

- 사물인터넷 홈네트워크 관련 안전성

사물인터넷 환경에서 홈네트워크 관련 블록체인 적용 기법의 효과 기기 연결에 대한 안전성과 사물인터넷에서 이용되고 있는 기기에 대한 사용 인증을 통하여 기밀성을 높일 수 있다. 홈 Wi-Fi의 해쉬 값을 IoT 기기에 보내 인증을 보낸 후, 보안인증을 한다. 해쉬값이 맞을 경우, 두 기기를 연결하도록 설계하여 무결성과 기밀성을

www.kci.go.kr

보장할 수 있다. 사용자가 IoT 기기를 사용 등록을 할 때 공격자가 사용자의 애플리케이션을 해킹하여도 어떠한 기기를 사용하는지 알 수 없도록 기밀성을 보장하여 안전성을 높이고 있다.

5. 결론

4차 산업혁명으로 발전하면서 발생할 위험이 가장 높은 의료정보, 지능형 자동차, 사물인터넷 기반의 홈네트워크에 대한 보안 위협요소들을 살펴보고, 각각의 블록체인을 통한 기법을 제안하였다. 특히 프라이빗 블록체인의 개방성은 비교적으로 약하지만 기존의 시스템을 보았을 때 저장 정보의 다양성과 빠른 처리 속도의 성능을 가지고 있어 기법에 적용하도록 하였다. 또한 의료정보에서는 허가 받은 소수 이용자만 참여하기 때문에 열람 권한에 제한을 두어 기밀성만큼은 뛰어나다고 말할 수 있다. 의료정보는 환자의 개인, 의료정보 등을 담고 있기 때문에 민감하고 예민하고 신경을 많이 써야한다. 그렇기 때문에 의료정보 시스템들을 프라이빗 블록체인을 사용하여 개인의 정보를 보호하고 기밀성을 유지하여 허가된 사용자들에게만 공유할 수 있도록 한다. 비록 프라이빗 블록체인의 단점인 허가된 사용자들에게만 공유할 수 있도록이라는 부분에 있어서 가끔씩은 다른 사람들도 볼 수 있도록 허가를 승인을 해야하는 불편함이 있겠지만 이를 보안할 수 있는 기술을 다음에 추가적인 연구가 필요하다. 지능형 자동차의 문제점을 해결해 나가는 정보보호 기법을 제안하였고 안전성을 높여 문제점을 벗어나고자 하였다. 제안한 시스템은 기존의 시스템과는 다른 블록체인의 기술을 이용하여 데이터를 블록화하고 요구사항들을 분석하는 기술을 접목시킴으로써 지능형 자동차에 대한 보안 기술 및 대응방안을 얻기를 기대하고 많은 발전의 가능성을 생각하며 연구가 이루어질 것이라 보고 앞으로 지능형자동차의 여러 기술들이 적용될 것이라고 생각한다. 사물인터넷에서 홈네트워크는 다양한 홈 디바이스를 통한 심각한 보안 문제점을 갖고 있기 때문에 이를 해결할 수 있는 방안이 필요하여 블록체인의 특성을 이용하여 보완하는 방법과 기법을 제안하였다. 이를 활용하면 스마트 홈 및 사용자들이 사용하고 있는 IoT 기기들을 안전하게 사용할 수 있을 것이며, 해커로부터의 해킹이나 사생활 침해를 막을 수 있을 것이다. 3가지의 제안 내용의 기법을 통하여 향후에는 좀더 구체적인 프로토콜을 제안하여 보안에 대한 확정성을 높이는 연구가 필요하다.

REFERENCES

[1] E.G.Hong, S.J.Lee and S.H.Seo, "Blockchain Technology Trends for the Internet of Things", Journal of Information Security, Vol.9, No.1, pp.38-46, 2018.

[2] J.H.Choi, K.H.Lee and S.H.Yun, "Abnormal Process Detection Using Blockchain", The Korea Internet of Things Society Comprehensive Conference 2019, Vol.4, No.1, pp.67-68, 2019.

[3] H.Y.Kim, "Analysis of Security Threats and Countermeasures on Blockchain Platforms," Korean Institute of Information Technology, Vol.16, No.5, pp.103-112, 2018.

[4] H.J.Chu, I.H.Song and B.G.Choi, "A Decentralized Test Management Tool Based on Blockchain Technique," The Korean Institute of Information Scientists and Engineers, Vol.25, No.7, pp.321-328, 2019.

[5] J.H.Hong, K.H.Lee and S.H.Yun, "A Scheme for ECU Application Technique using Blockchain", The Korea Internet of Things Society Comprehensive Conference 2019, Vol.4, No.1, pp.34-35, 2019.

[6] Hyperledger Architecture, Volume 1, https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf, 2018.

[7] J.H.Yoon and M.H.Kim, "Private blockchain and smart contract-based high reliability crowd sensing compensation mechanism". Journal of Information Security and Cryptology, Vol.28, No.4, pp.999-1007, .2018.

[8] M.J.Jung, K.H.Lee and S.H.Yun, "Design of Medical Information Security System Using Blockchain", The Korea Internet of Things Society Comprehensive Conference 2019, Vol.4, No.1, pp.40-41, 2019.

[9] J.T.Lee, "Identify key issues and analyze future development directions through analysis of technology and market trends in medical information systems.". Paper presented at the Korean Society for Intelligent Information Systems, pp.135-142, 2013.

[10] Y.K.Kim "Development Technics and Future Trend of Electronic Engine Control Unit," The Korean Society Of Automotive Engineers, Vol.19, No.2, pp.26-31, 1997.

[11] Y.S.Hong, "Evaluation of Function and Safety of Autonomous Vehicles," The Korea Transport Institute, pp.13-18, 2015.

[12] G.M.Lee, H.J.Cha and J.C.Kim "Model-based Design and Validation of ADAS Control Software on Multicore ECU," The Korean Society Of Automotive Engineers, pp.335-335, 2016.

[13] The Guardian, Woolf, N. "DDoS attack that disrupted internet was largest of its kind in history, experts say." [Internet], https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

www.kci.go.kr

[14] B.J.Park, T.J.Lee and J.Gwak, "Blockchain-Based IoT Device Authentication Scheme", Journal of the Korea Institute of Information Security and Cryptology, Vol.27, No.2, pp.343-351, 2017.

[15] K.W.Bae, K.H.Lee and D.H.Kim, "A Scheme for IoT Authenticatino Using Blockchain Forgery/Tamper Protection, The Korea Internet of Things Society Comprehensive Conference 2019, Vol.4, No.1, pp.46-48, 2019.

이 근 호(Lee, Keun Ho) [종신회원]

■ 2006년 8월 : 고려대학교 컴퓨터학과(이학박사)
■ 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
■ 2010년 3월 ~ 현재 : 백석대학교 ICT학부 부교수

〈관심분야〉
이동통신 보안, 융합보안, 개인정보보호

www.kci.go.kr