블록체인을 이용한 자동차 ECU 생체인증 기법

홍지훈[1], 이근호[2*]
[1]백석대학교 ICT학부 학생, [2*]백석대학교 ICT학부 교수

Automotive ECU Biometric Authentication Using Blockchain

Ji-Hoon Hong[1], Keun-Ho Lee[2*]
[1]Student, Div. of Information Communication, BaekSeok University
[2*]Professor, Div. of Information Communication, BaekSeok University

요 약 사물인터넷은 4차 산업혁명의 중요한 요소 기술로서 역할을 담당하고 있다. 본 연구는 최근 IT 기술을 적용한 지능형 자동차를 개발하고 있으며, 지능형 자동차에 대한 개발이 활발하게 이루어지면서 그에 대한 네트워크 데이터 통신이 가능하게 된 시점에 있다. 하지만 외부에서 네트워크에 침입하여 보안을 위협할 수 있으며 보안이 아직 미약한 단계이기에 그에 따른 보안솔루션이 필요하다. 본 논문에서는 지능형 자동차에 보안 문제가 발생하지 않고 보안성을 높이기 위해서 블록체인의 기술을 적용하고 사용자의 생체정보를 이용하여 생체인증 기법을 제안하고 향후 지속해서 연구하고자 한다.

주제어 : 블록체인, 지능형 자동차, 생체, 전자 제어시스템, 인증

Abstract The Internet of Things plays a role as an important element technology of the 4th Industrial Revolution. This study is currently developing intelligent cars with IT technology, and is at a time when the development of intelligent cars is active and network data communication is possible. However, security solutions are needed as security is still at a weak stage, which can be threatened by intrusions into the network from outside. In this paper, in order to improve security of intelligent cars without causing security problems, we will apply blockchain technology, propose biometric authentication techniques using users' biometric information, and continue to study them in the future.

Key Words : Blockchain, Intelligent Vehicle, Biometrics, Electronic Control Unit, Certification

1. 서론

최근 IT 기술이 발전하면서 그로 인하여 여러 분야에서 많은 기술이 발전하고 있으며, 이러한 기술로 인하여 자동차 분야에서도 적용하여 개발되고 있다. 지능형 자동차에 대한 인터페이스가 개발되면서 보안 문제가 제기될 수 있는데, 현재 지능형 자동차에서 스마트폰과 ECU를 연동하여 모바일 네트워크, 근거리 무선통신망, 블루투스 등을 접속할 수 있는 기술이 개발되면서 애플리케이션으로 직접 차량과 연결하여 사용자의 자동차 정보를 확인할 수 있고 그에 따른 바이러스나 해킹 공격이 발생하여 취약할 수밖에 없다.

해킹 공격으로 인하여 자동차 시스템을 해킹하여 시스템의 문제가 생긴다면 운전자의 생명을 위협하고 개인정보 노출과 위치 파악으로 인한 사생활 문제로 이어질 수 있기에 이를 막기 위하여 보안솔루션이 필요하다. 이러한

본 논문은 2020년 백석대학교 학술연구에 의하여 지원되었음
*교신저자 : 이근호(leekeunho1004@gmail.com)
접수일 2020년 2월 20일 수정일 2020년 3월 10일 심사완료일 2020년 3월 23일

자동차의 정보 조작 및 민감한 데이터 노출을 막고자 사용자의 생체인증을 사용하고 블록체인 기술을 이용하여 기존 지능형 자동차에 적용하고 사용자 차량을 분별하여 외부에서 접근하는 것을 제안 할 수 있도록 기존 논문에서 더 발전하여 목표로 한다[1].

현재 시스템과 연동되는 서비스는 간단한 인증으로만 접근하는 방법을 사용하고 있어 쉽게 공격을 당할 수 있기에 이러한 문제점에 대한 보안솔루션으로 두 기술을 적용하여 새로운 보안솔루션을 제안하고자 한다.

2. 관련연구

2.1 전자 제어시스템 및 위협

전자 제어시스템(ECU)은 장치로 자동차의 모든 전자 제어를 전자적으로 관리하며 자동차가 제어하는 엔진, 변속기, 조향, 제동, 현가장치 등을 제어하는 장치로 기존의 목적과는 다른 기술이 발전하면서 기술을 많아지고 ECU가 제어하는 기능들이 점차 많아지고 있다[2.3]. 모든 동작을 제어하고 관리하는 역할을 하고 지능형 자동차에서 제일 중요한 장치이다[4]. ECU는 크게 입력, 출력, 연산으로 나눠서 구분할 수 있으며 입력은 출력값을 보고 연산과 출력은 제어장치의 제어를 보고 있다[5].

보안솔루션이 간단하게 비밀번호를 이용하여 자동차 시동과 위치추적이 가능한데 이러한 보안솔루션으로 한계가 있어 사용자의 차량 정보가 노출되거나 비밀번호를 도난당할 수 있기에 그에 따른 문제점이 발생 할 수 있다[6,7.8]. 따라서 ECU와 연동해서 이루어지는 환경에서 다양하게 개발하고 상용화를 위해서 보안시스템의 문제점을 해결할 방안이 필요하다.

2.2 블록체인

블록체인이란 데이터의 변조를 판단하기 위하여 정보들을 모아 블록의 해시를 만들고 해시를 생성할 때마다 이전 블록의 해시값을 입력하여 현재의 블록 해시를 만들어 영향을 끼치게 한다. 블록체인은 중앙관리체제로 운영되는 클라우드와 비교되는 네트워크의 구조이면서 분산형 구조 형태로 모든 데이터의 정보를 가지고 있다. 중앙서버에서 모든 정보를 처리하는 클라우드 방식과는 다른 네트워크 방식으로 동작한다[9.10].

데이터 정보를 하나에 블록에만 저장하지 않고 여러 곳으로 분산하여 분산된 형태로 배치하고 저장하기 때문에 데이터가 변조될 가능성은 매우 낮아 중앙서버에서 관리하는 형태가 아니기 때문에 사용자의 모든 데이터의 정보를 가지고 있다. 중앙체제에서는 서버에 저장한 정보를 보호하기 위하여 시스템들을 보안하고 운영한다. 그러므로 정보를 서버에 저장하는 방식 및 보안에 필요한 인력이 적기 때문에 유지하는 비용이 적게 된다. 블록체인의 방식은 중앙 관리체제가 필요하지 않은 방식이라서 서버에서 소모되는 비용은 적게 된다[11,12].

2.3 M2M을 이용한 인증기법

M2M(Machine to Machine)은 기계 간의 통신이며 즉 디바이스와 기계 간의 통신이다. ECU의 제어하는 모든 동작을 사용자 생체정보로 이용하여 접근하는 인증기법으로 제안한다. 또한, 내부 네트워크에 접근하기 위해서 생체인증을 통하여 인증을 받은 후 접근하는데 신체정보의 센서가 부착된 단말기, 바이오센서, NFC(Near Field Communication) 등을 통하여 진행한다[13,14]. ECU 제어장치로 이동하기 위한 많은 정보를 입력해야 하는데 이러한 정보를 사물 통신으로 전송하기 때문에 트래픽이 가벼워야 한다. 데이터 정보를 숨김으로써 기밀성과 동시에 트래픽을 절약을 할 수 있다[15].

3. 보안 위협요소 시나리오

기존의 지능형 자동차의 보안솔루션은 간단하게 PW를 통하여 인증으로 차량의 시동과 위치정보를 볼 수 있고 ECU와 스마트폰이 M2M 통신을 하는 방식이었다. 하지만 PW를 이용한 솔루션은 한계가 있어 비밀번호를 도난당하거나 노출되었을 경우 사용자의 차량 정보가 유출될 수 있기에 그에 맞는 보안의 위협이 발생할 수 있기에 완벽하다고 말할 수 없다. 그러므로 차량 ECU와 연동해서 이루어지는 환경에서 다양한 기술을 적용하여 이러한 문제점을 해결할 효율적인 방안이 필요하다.

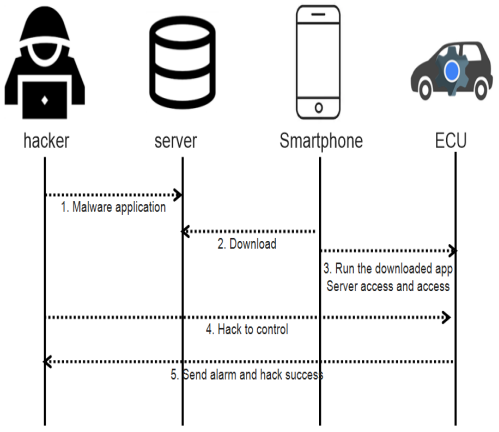
3.1 애플리케이션

차량의 발전으로 효율적으로 관리가 이루어지고 있는데 최근 IT의 발전으로 인해 ECU를 장착하는 차량이 많이 생겨나고 있다. 전자제어 시스템을 통해 엔진의 동력 및 에어백, 브레이크, 제동 등의 상태나 동작하는 데이터를 실시간으로 확인하여 차량을 점검 할 수 있다. 또한, 점검된 차량의 정보를 블루투스로 실시간 업데이트를 진

행하여 메모리에 저장하고 있다. 만약 이렇게 저장한 데이터들이 노출된다면 많은 문제가 발생하게 된다.

3.2 취약점을 이용한 공격

현재 발전이 이루어지고 있는 자동차의 분야는 아직 보안이 취약한 부분이 있기에 많은 보안의 위협이 생겨나고 있다. 아래의 [Fig. 1]은 그러한 내용을 가지고 시나리오를 작성한 것이다.



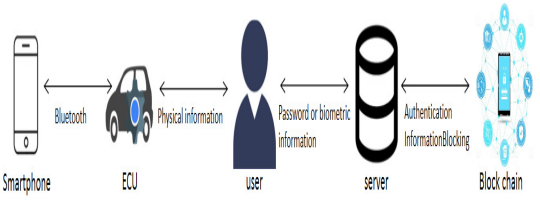
[Fig. 1] ECU Hacking Scenario

step 1 : 해커는 서버에 악성코드로 제작한 애플리케이션을 올린다.
step 2 : 사용자는 애플리케이션을 다운로드 하여 사용하게 된다.
step 3 : 다운로드 한 애플리케이션을 네트워크를 이용하여 실행하게 된다.
step 4 : 해커는 자신의 서버로 접속하고 네트워크를 연결한 차량의 ECU 접근한다.
step 5 : 해커는 접근한 차량의 제어 시스템을 해킹하고 접근하게 된다.
step 6 : 성공한 해커는 운전 중인 사용자의 핸드폰의 알림을 띄우고 해킹을 성공하게 된다.

취약한 내부 네트워크를 통하여 악성코드를 감염시킨 스마트폰을 자동차와 연결하게 되면 쉽게 제어 시스템에 접근할 수 있게 된다. 또한, 제어를 할 수 있기에 공격자는 차량의 시스템을 무선으로 제어하게 되어 많은 문제가 발생하게 된다.

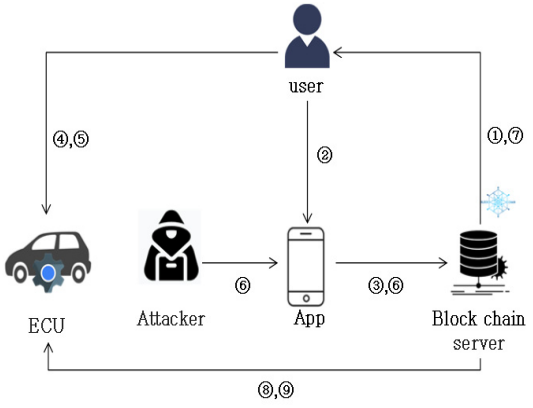
4. 제안기법

기존 사용자의 인증을 위해서는 패스워드나 서버로 이용했으나 블록체인을 이용하여 사용자의 개인정보 위변조를 방지하고 관리시스템에서 벗어나 새로운 인증기법으로 아래 [Fig. 2]로 제안한다.



[Fig. 2] New Vehicle Authentication Techniques

제어 시스템에서 사용하는 인증 방식을 블록체인의 기술을 적용하여 생체인증 및 인증하는 데이터를 블록화하고 높은 보안성을 가지게 된다. 만약 다른 방식으로 자율주행 자동차를 관리하는 서버를 해킹 공격이 들어오게 되더라도 블록화된 데이터를 열어 볼 수 없다.



[Fig. 3] Model with Blockchain and Biometrics.

step 1 : 서버에서는 사용자에게 생체정보를 등록 및 주기적인 업데이트를 요구한다.
step 2 : 사용자는 수시로 생체정보 및 핸드폰을 업데이트하여 자동으로 데이터값이 서버에 전송이 된다.
step 3 : 서버에서는 생체정보 데이터를 받아 블록화하여 저장하고 분석하여 전송한다.
step 4 : 사용자는 차량 시스템을 업데이트하여 주기적으로 로그를 서버에 전송하고 새로운 사

용자가 있으면 사전 등록을 하게 된다.

step 5 : 만약에 실시간으로 침입 탐지가 발견되면 분석을 하여 차량을 점검받게 하고 로그를 남긴다.

step 6 : 공격자가 악성코드로 제작한 애플리케이션을 등록하고 사용자가 실행하게 되면 공격자는 서버에 접속하여 데이터를 훔치게 된다.

step 7 : 서버에서 공격을 감지하게 되면 사용자에게 생체인식을 요구하게 되고 생체인식 값과 저장된 값이 틀리면 공격으로 감지하게 된다.

step 8 : 서버에서는 ECU에 신호를 보내 즉시 차량의 자율주행 시스템을 정지하고 수동으로 운전자에게 넘겨주게 된다.

step 9 : 실시간으로 데이터를 공유하면서 사전 문제점을 차단하고 예방한다.

5. 기대효과

기존 시스템과 새로운 시스템을 비교하였다. 기존 시스템에서 보안의 위험이 발생할 수 있기에 새로운 기술을 적용하여 보안성을 강화하고 상황에 따른 판단력을 가지게 된다. 또한 기존 방식의 데이터관리보단 효율적으로 데이터를 관리하여 공격위험에서 벗어나고 안정성을 가지게 되는데, 공격이 발생하더라도 완전한 공격이 아니게 되어 효율적인 관리가 이루어진다. 기존 기능 성능도 좋지만, 더욱 기술을 적용하게 된다면 더 좋은 기대효과를 가지게 될 것으로 생각한다.

〈Table 1〉 System performance comparison

system / Component	Existing system	New system
Efficiency	Normal	good
Danger	high	Normal
Performance	good	very good
Security	Normal	very good
data management	Normal	good
Situation judgement	Normal	good

6. 결론

본 논문에서는 기존의 보안솔루션보다 높은 보안성을 가지기 위해 지능형 자동차의 문제점을 해결하고 앞으로 더 좋은 기술로 적용하여 지금보다 문제점을 해결하고 나가는 블록체인을 활용하여 시스템을 제안하였다. 제안한 인증시스템은 기존 시스템과는 다르게 차량 내부 네트워크에 접근하기 위해 사용자 생체정보를 기반으로 한 프로세스를 통하여 생체정보는 고유의 암호가 될 수 있으며 블록체인의 기술을 이용하여 데이터를 블록화하고 요구사항들을 분석하여 접목하게 시키면서 지능형 자동차에 대한 보안 기술이나 대응 방안을 얻기를 기대하고자 많은 발전의 가능성을 생각하면서 연구가 이루어질 것으로 생각한다. 또한, 앞으로 지능형 자동차의 여러 기술이 적용될 것으로 생각하면서 제안하였다.

REFERENCES

[1] J.H.Hong, K.H.Lee and S.H.Yun, “A Scheme for ECU Application Technique using Blockchain,” Korean Society of Internet Science, Vol..4, No.1, 2019.

[2] 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.

[3] H.C.Moon and J.H.Kim, "Electronic Control System for Vehicle Performance Improvement," Journal of Institute of Control, Robotics and Systems, Vol.16, No.2, pp.20-25, 2010,

[4] Y.S.Hong, “Evaluation of Function and Safety of Autonomous Vehicles,” The Korea Transport Institute, Vol.11, No.12, pp.13-18, 2015.

[5] G.M.Lee, H.J.Cha, J.C.Kim, “Model-based Design and Validation of ADAS Control Software on Multicore ECU,” The Korean Society Of Automotive Engineers, Vol.2016, No.11, pp.335-335, 2016.

[6] J.H.Ahn and Y.H.Kim, “Implementation of Android Application for Intelligent Vehicles,” Korea Institute of Information Technology Summer Conference, Vol.2011, No.5, 2011.

[7] S.H.Baek, J.G.Kim, S.H.Park and H.T.Ju, “A Development of a Trip computer based on Android,” Journal of Korean Information Science Society, Vol.37, No.2B, pp.397-400, 2010

[8] H.R.Lee, K.J.Kim, K.H.Jung, K.H.Chio, S.K.Park and D.K.Kwon, “Studies of the possibility of external threats of the automotive ECU through simulation test environment,” Journal of the Korea Society of Computer and Information, Vol.18, No.11, pp.39-49, 2013

[9] Y.S.Kim, Y.C.Kim and B.Y.Lee, “Security Model Tracing User Activities using Private BlockChain in Cloud Environment,” The Journal of the Korea Contents Association, Vol.18, No.11, pp.475-483, 2018.

[10] K.H.Lee, “A Scheme on Anomaly Prevention for Systems in IoT Environment ,” Journal of the Korean Society for Internet of Things, Vol.5, No.2, pp.95-101, 2019.

[11] H.Y.Kim, “Analysis of Security Threats and Countermeasures on Blockchain Platforms,” Korean Institute of Information Technology, Vol.16, No.5, pp103-112, 2018.

[12] 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.

[13] J.O.Hwang and S.G.Lee, “Study on the 3GPP International Standard for M2M Communication Networks,” The Journal of Korean Institute of Communications and Information Sciences, Vol.40, No.6, pp.1040-1047, 2015.

[14] N.S.Kim, “Hybrid Spectrum Sensing System for Machine-to-Machine(M2M),” The Journal of Korea Institute of Information, Electronics, and Communication Technology, Vol.10, No.2, pp.184-191, 2017.

[15] J.H.Song and S.S.Kim and M.S.Jun, “A Study on Group Key Generation and Exchange using Hash Collision in M2M Communication Environment,” The Journal of The Institute of Internet, Broadcasting and Communication (IIBC), Vol.19, No.5, pp.9-17, 2019.

홍 지 훈(Hong, Ji Hun) [학생회원]

- 2014년 3월 ~ 현재 : 백석대학교 ICT학부

〈관심분야〉
영상처리, 개인정보보호,

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