산업융합연구 제20권 제11호 pp. 57-63, 2022
ISSN 2635-8875 / e-ISSN 2672-0124
DOI : https://doi.org/10.22678/JIC.2022.20.11.057

블록체인을 활용한 ECU 데이터 무결성 검증 시스템

변상필[1], 김호윤[2], 신승수[3*]
[1]동명대학교 정보보호학과 학생, [2]동명대학교 컴퓨터미디어공학과 학생, [3]동명대학교 정보보호학과 교수

ECU Data Integrity Verification System Using Blockchain

Sang-Pil Byeon[1], Ho-Yoon Kim[2], Seung-Soo Shin[3*]
[1]Student, Dept. of Information Security, Tongmyong University
[2]Student, Dept. of Computers & Media Engineering, Tongmyong University
[3]Professor, Dept. of Information Security, Tongmyong University

요 약 자동차의 센서, 신호 등 데이터를 수집·처리하는 ECU 데이터가 공격에 의해 조작되면 운전자에게 피해를 줄 수 있다. 본 논문에서는 블록체인을 이용하여 자동차 ECU 데이터의 무결성을 검증하는 시스템을 제안한다. 자동차와 서버는 세션 키를 이용해 데이터를 암호화하여 송·수신하기 때문에 통신 과정에서 신뢰성을 보장한다. 서버는 해시 함수를 이용해 전송받은 데이터의 무결성을 검증한 후, 데이터에 이상이 없으면 블록체인과 off-chain인 분산저장소에 저장한다. ECU 데이터 해시값은 블록체인에 저장하여 변조할 수 없으며, 원본 ECU 데이터는 분산저장소에 저장한다. 해당 검증 시스템을 이용해 ECU 데이터에 대한 공격 및 변조를 사용자가 검증할 수 있으며, 악의적인 사용자가 ECU 데이터에 접근하여 데이터 변조 시 무결성 검증을 수행할 수 있다. 보험, 자동차 수리, 거래 및 판매 등의 상황에서 사용자의 필요에 따라 사용할 수 있다. 향후 연구로는 실시간 데이터 무결성 검증을 위한 효율적인 시스템 구축이 필요하다.

키워드 : 전자제어장치, 커넥티드카, 블록체인, 분산형 파일 시스템, 무결성

Abstract If ECU data, which is responsible for collecting and processing data such as sensors and signals of automobiles, is manipulated by an attack, it can cause damage to the driver. In this paper, we propose a system that verifies the integrity of automotive ECU data using blockchain. Since the car and the server encrypt data using the session key to transmit and receive data, reliability is ensured in the communication process. The server verifies the integrity of the transmitted data using a hash function, and if there is no problem in the data, it is stored in the blockchain and off-chain distributed storage. The ECU data hash value is stored in the blockchain and cannot be tampered with, and the original ECU data is stored in a distributed storage. Using the verification system, users can verify attacks and tampering with ECU data, and malicious users can access ECU data and perform integrity verification when data is tampered with. It can be used according to the user's needs in situations such as insurance, car repair, trading and sales. For future research, it is necessary to establish an efficient system for real-time data integrity verification.

Key Words : Electronic control unit, Connected car, Blockchain, Interplanetary files system, Integrity

1. 서론

ICT 기술이 발달하면서 자동차 분야에서도 네트워크 통신 기술이 급속히 발전하고 있다. 자동차 기술은 자율주행 자동차, 커넥티드 카 등 지능형 자동차의 형태로 지속적인 개발이 이뤄지고 있다[1]. 자율주행은 주행 과정에 있어서 운전자의 개입 없이 자동차가 스스로 목적지까지 주행하는 기술을 의미하며 자동화 수준에 따라 6단계로 분류된다.

커넥티드카는 차량에 무선 랜을 장착하여 차량과 차량

This research was supported by the BB21plus funded by Busan Metropolitan City and Busan Institute for Talent & Lifelong Education(BIT).
*Corresponding Author : Seung-Soo Shin(shinss@tu.ac.kr)
Received August 2, 2022 Revised September 2, 2022
Accepted November 20, 2022 Published November 28, 2022

(V2V: Vehicle-To-Vehicle), 차량과 인프라(V2I : Vehicle-To-Infrastructure), 그리고 차량과 모든 장비 (V2X: Vehicle-To-Everything) 형태로 차량의 내·외부로 네트워크가 연결된 차량을 의미한다[2].

자동차는 전기 · 전자 시스템 비중이 급격하게 늘어나고 있으며, 대표적으로 지능형 자동차에서는 자동차의 제어를 담당하는 전자제어장치(ECU : Electronic Control Unit)가 있다. ECU는 자동차에 제어 신호를 출력하여 통제하는 장치로서 이용자는 네트워크 기기와 연결하여 애플리케이션을 통해 정보를 확인하고, 자동차의 상태정보를 손쉽게 확인할 수 있다. 자동차는 전기·전자화된 형태로 발달하면서 보안 측면에서 자동차의 ECU 데이터에 대한 안전성 및 신뢰성이 보장되지 않는다면 악의적인 공격자가 자동차의 정보를 탈취하여 ECU의 동작 및 데이터 처리에 영향을 끼쳐 탑승자에게 물리적인 피해를 줄 수 있다[3].

차량의 정비 및 거래에 있어서 데이터 조작을 통해 불법적인 이득을 취하거나 악용할 가능성도 있다. 친환경 정책에 따라 고연비 및 배기가스의 저감 실현을 위해 매연 저감장치를 조작하거나, 대기오염 물질 배출 절감을 위한 요소수 대란으로 인해 가격이 폭등하자 저감장치를 조작한 사례도 있다[4]. ECU 데이터에 대한 공격 및 조작을 방지하고 신뢰성을 보장하기 위해서 데이터의 무결성을 검증하는 기술은 필수적이며 최근에는 공격자의 ECU 접근 방지를 위해 시큐어 플래시, 접근 제어 등의 기술이 있다.

본 논문에서는 지능형 자동차에서 ECU 데이터에 대한 조작 및 공격을 막기 위하여 수집된 차량 데이터들을 블록체인에 저장, 관리하여 ECU 데이터 무결성 검증 시스템을 제안한다. 블록체인을 이용하여 차량 데이터를 관리하기 때문에 ECU 데이터의 무결성을 검증할 수 있으며 ECU 데이터의 원본은 오프체인(off-chain) 방식을 이용해 외부의 분산저장소에 별도로 보관한다. 기존의 ECU 데이터는 전문 업체를 찾아 데이터를 검증해야 하지만 제안하는 시스템을 통해 사용자는 저장된 ECU 데이터에 접근하기 편리하며, 불법적인 조작에 대한 검증을 손쉽게 할 수 있다. 사용자가 차량 데이터가 필요할 경우 검증된 데이터를 이용해 자동차의 수리, 거래 및 사고가 발생했을 경우 필요에 따라 다양한 용도로 사용할 수 있다.

2. 관련 연구

ECU는 자동차의 내부 네트워크를 통해 서로 통신하면서 데이터를 주고받기 때문에 이와 관련된 동향과 연구에 대해서 알아본다.

2.1 전자제어장치

ICT 기술이 발전함에 따라 다양한 기술들이 개발되고 빠른 속도로 발전하고 있다. 이러한 기술 발전들은 자동차 분야에서도 적용이 되고 있다. 자동차의 ECU는 과거 엔진제어 장치로만 표현되었으나 차량의 전자화가 이뤄짐에 따라 차량 내에 있는 각종 센서를 통해 데이터를 수집하고, 수집된 데이터를 분석하여 제어 신호로 출력하는 일종의 임베디드 시스템을 의미한다. 자동차 기술이 발전하면서 전·후방 카메라, 라이다(LIDAR) 센서, O2 센서, 차속 센서, 크랭크 센서 등으로부터 데이터를 수집한다. ECU는 30개에서 많게는 100개 정도까지 차량에 장착되고 이는 ECU가 제어, 관리하는 기능이 많아지고 있음을 의미한다. ECU의 구성은 Fig. 1과 같다[5-7].

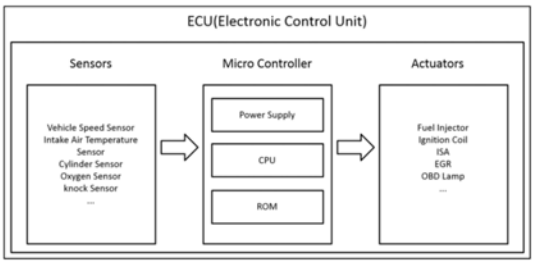

Fig. 1. ECU component

자동차 기술이 발전함에 따라 더 많이 ECU가 장착될 것이다. 장착되는 ECU의 수가 증가하는 것은 전자적으로 제어되는 영역이 증가한다는 것을 의미하고 이는 차량 데이터의 신뢰성 및 안전성 또한 중요해진다는 것을 의미한다. ECU를 통해 수집된 데이터가 악의적인 사용자에게 넘어가 운전자의 생명을 위협할 수 있고, 차량 수리 및 거래 데이터를 가진 사용자가 정보를 조작하여 악용할 가능성이 있다.

2.2 자동차 네트워크 기술

ICT 기술이 발전하고 자동차 분야에 적용됨에 따라 많은 ECU가 자동차에 장착되는데 이로 따라 복수의 ECU를 제어하기 위해 자동차 내 네트워크(IVN : In- Vehicle Network)가 필요하다. IVN 기술은 ECU의 성능이 발전함에 따라 더 많은 연산과 다량의 데이터를 송수신하게

되며 전체적인 데이터 송·수신량의 증가 및 데이터 연산에 있어서 저 지연 및 고신뢰성을 요구하여 자동차 내부의 네트워크의 속도, 전송량 및 신뢰성 등의 역할이 중요하다. 이에 따라 LIN(Local Interconnect Network), CAN(Controller Area Network), FlexRay, 차량용 이더넷 등 다양한 차량 네트워크가 개발되었다[8,9].

V2X 통신기술로는 WAVE(Wireless Access in Vehicular Environment) 무선 통신 기술과 3GPP에서 표준화된 C-V2X(Cellular-V2X) 기술이 있다. WAVE 통신은 지국과 코어 네트워크를 통하지 않고 자동차 간 직접 통신(V2V)이 가능하고 응답시간이 100ms 이내로 짧고 고속이동 중에도 통신이 가능하다는 특징이 있다. 하지만 짧은 전송 거리와 낮은 속도로 인해 제한적인 구현이 가능하다는 한계점이 있다.

C-V2X는 Cellular 네트워크를 기반으로 하여 통신하는 방식이다. 2017년 3월에 3GPP LTE Release 14에서 표준으로 발표되었으며, 이후 기본 틀을 유지하면서 지연을 줄이고 향상한 C-V2X 표준이 Release 15에서 발표되었다. 그리고 2020년에 초저지연, 고 신뢰성 및 초고속을 지원하는 5G 기술을 이용한 NR -V2X가 있다[10,11].

차량 통신은 일반적인 네트워크와 달리 노드가 고속이동하기 때문에 네트워크의 링크 연결이 짧다. 따라서 패킷 손실률은 높고 네트워크의 연결이 불안정하므로 자율주행을 위한 자동차 통신기술을 구현하기 위해서는 기존의 통신 서비스와 호환이 되어야 하고, 초고속 데이터 전송 속도, 낮은 지연시간 및 신뢰성을 보장해야 한다[12].

2.3 ECU 데이터 조작 및 공격 사례

데이터를 블록체인에 저장하기 위해 자동차와 서버는 통신이 원활해야 하며 이를 위해 자동차의 네트워크에 관련된 기술이 활발히 연구되고 있다. ECU 데이터의 무결성을 검증하는 시스템을 제안하기 이전에 ECU 데이터의 조작 및 공격에 대해 과거에 발생했었던 사례에 대해 알아본다.

악의적인 사용자는 ECU 데이터 조작으로 불법적인 이득을 취할 수 있다. 배출가스양을 조작하거나, 매연 저감 장치의 조작 및 속도 제한의 상한선을 올리는 등의 조작이 가능하다. 해외에서는 2015년 폭스바겐이 디젤 차량에 배출가스의 감사결과를 조작하는 소프트웨어를 설치하여 배기가스 기준치의 30배의 배기가스가 발생한다는 사실을 숨겼다[13].

국내에서는 경유차에 배기가스 규제로 인해 선택적 촉매환원 장치를 장착해야 하며, 이 장치는 요소수가 필요하다. 2021년 요소수 가격이 폭등하자 차주들은 ECU의 불법 개조를 통해 소량의 요소수로 운행할 할 수 있도록 개조한 사례가 있다[14].

ECU 공격사례는 다음과 같다. ECU는 자동차 내부에서 CAN(Controller Area Network)이라 불리는 통신 프로토콜을 사용하고 있다. 자동차 내부에 CAN 데이터 프레임을 주입하여 ECU의 조작을 통해 자동차의 원격제어가 가능하며, ECU 장치의 지연 및 동작을 중단시켜 자동차 주행에 영향을 끼칠 수 있다[15].

공격자는 대상 자동차의 ECU를 외부에서 접근하여 ECU 메모리 조작, 보안 키를 변조할 수 있으며 ECU의 펌웨어를 공격자가 지정한 펌웨어로 플래시하여 악의적으로 이용할 수 있다. 공격자가 ECU에 접근하여 악의적인 행동을 하지 못하도록 하는 것은 자동차 보안에 있어서 중요하며 이를 위해 자동차 통합 진단 표준 및 HSM 기반의 ECU 보안 플랫폼 규격 등 자동차 관련 보안 기술이 표준화되고 있으며 ECU 보안을 위한 기술로는 시큐어 플래시, 접근 제어 등이 있다[16].

3. ECU 데이터의 무결성 검증 시스템

자동차는 빠른 기술 발달에 맞춰 전기·전자화되며 함께 발전하고 있다. 따라서 ECU의 역할은 커지고 있으며, 자동차 ECU 데이터에 대한 공격 및 조작에 대한 대안으로 블록체인에 기반 한 ECU 검증시스템을 제안한다. 제안한 시스템을 이용하여 자동차의 주요 데이터를 안전하게 송·수신하여 보관할 수 있으며 자동차의 데이터를 다양한 환경에서 활용할 수 있다.

3.1 시스템 구성

ECU 데이터의 무결성 검증 시스템은 자동차 ECU, 서버, 블록체인 네트워크, 그리고 분산저장소(DFS : Distributed File System)로 구성된다. 시스템의 구성은 Fig. 2와 같다.

제안한 시스템 모델에서 자동차 ECU는 자동차의 주행 과정에서 다양한 센서들로부터 데이터를 수집하여 분석한 후, 제어신호로 출력하여 자동차 제어에 관여하는 역할을 한다. 센서들로부터 수집된 ECU 데이터들은 자동차 제어를 위한 중요한 데이터이기 때문에 위조 및 변조 등의 공격에 대응할 수 있어야 한다.

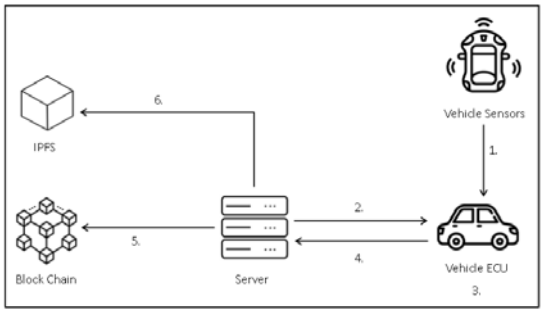

Fig. 2. System model

서버는 자동차와 데이터를 송·수신하여 무결성을 검증한 후, 데이터를 블록체인 네트워크 및 분산저장소로 전송하는 역할을 한다. 블록체인 네트워크를 사용하여 ECU 데이터의 무결성을 보장하고 검증을 마친 해시값을 저장한다. 블록체인에 데이터의 해시값을 저장하여 사용자가 불법적인 데이터 조작을 할 수 없도록 하며 작은 크기의 데이터로 무결성을 검증할 수 있다. ECU 데이터는 블록체인 네트워크에서 각 블록의 최대 크기에 대한 문제 및 모든 ECU 데이터 내용을 블록체인에 참여한 모든 참여자가 보유하게 된다는 문제점을 방지하기 위해서 off-chain 방식을 사용하여 외부의 분산저장소에 별도로 저장한다.

분산저장소에 보관되는 데이터는 무결성 검증 역할 이외에도 데이터를 활용하여 사용자에 따라 차량 정비, 판매, 보험 등 다양한 상황에서 사용될 수 있다.

3.2 무결성 검증 시나리오

제안한 시스템 모델에서 ECU 데이터의 무결성 검증을 위한 시나리오는 다음과 같다.

첫 번째, 자동차 ECU 데이터의 수집 과정은 다음과 같다. ECU는 자동차 내에 있는 센서들로부터 데이터를 수집 및 가공하여 자동차를 제어하는 신호로 출력한다. 센서는 흡입 공기량 검출, 수온, 흡기 온도 및 산소 등 다양한 요소들로부터 데이터를 수집하며 이를 ECU에서 처리를 통해 연료 분사량, 분사 시기 및 공연비 등 차량의 제어에 관여한다.

두 번째, 자동차 ECU 데이터의 암호화 및 전송 과정은 다음과 같다. 자동차는 서버가 생성한 세션키를 자동차의 공개키로 암호화하여 전송하면 암호화된 세션키를 전송받은 뒤, 자동차의 개인키를 이용하여 세션키를 복호화한다. 그리고 자동차는 서버로부터 발급받은 세션키를 이용하여 수집된 데이터를 암호화한 후 서버로 전송한다.

세 번째, 서버가 ECU 데이터의 무결성을 검증하는 과정은 다음과 같다. 자동차는 ECU 데이터의 해시값을 계산한 뒤 발급받은 세션키를 이용해 ECU의 데이터와 해시값을 암호화하여 서버로 전송한다. 서버는 전송받은 해시값과 ECU 데이터를 복호화한 후, 서버는 ECU 데이터의 해시값을 생성하여 전송받은 해시값과 비교한 뒤 해시값의 무결성을 검증한다.

네 번째, 검증을 완료한 ECU 데이터의 등록 과정은 다음과 같다. 서버는 무결성 검증을 완료하면 ECU 데이터의 해시값은 블록체인에 등록하여 저장하고 ECU 데이터의 원본은 off-chain인 IPFS (InterPlanetary File System)에 저장한다. 이때 IPFS 접근 해시값 또한 블록체인 네트워크에 같이 저장한다. 제안한 시스템의 무결성 검증 시나리오는 Fig 3과 같다.

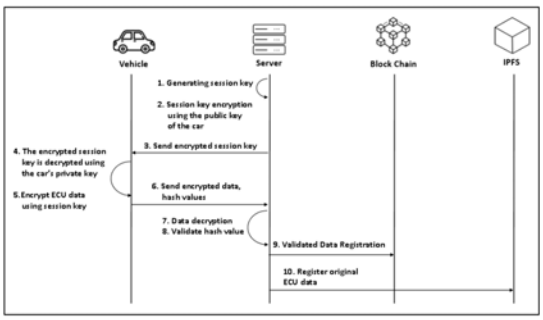

Fig. 3. System scenario

3.3 시나리오 검증

제안하는 시스템은 블록체인과 분산저장소를 이용해 데이터를 저장한다. 블록체인은 Hyperledger Fabric을 이용해 구현하고, 분산저장소는 IPFS를 이용해 구현한다. 시나리오 검증에서는 블록체인과 분산저장소에 데이터를 저장하는 환경을 구현한다. 구현 환경은 Table 1과 같다.

Table 1. Software development environment

Classification	Specification
Operation System	Ubuntu 20.04.3 LTS
Environment	Virtual Box
Platform	Hyperledger 1.4.11, Docker 20.10.14
Dev language	Python 3.8.10, Go 1.16.15
Distributed file system	IPFS 0.4.17

서버는 자동차로부터 받은 ECU 데이터와 해시값을 검증한 후 이상이 없다면 ECU 데이터는 IPFS로 전송하고

해시값은 블록체인 네트워크로 전송하여 저장한다. 이때 해시값을 저장하는 블록체인 네트워크의 체인코드는 Fig. 4와 같다.

```
func (s *SmartContract) Init(APIstub shim.ChaincodeStubInterface) pb.Response {
    return shim.Success(nil)
}
func (s *SmartContract) Invoke(APIstub shim.ChaincodeStubInterface) pb.Response {
    function, args := APIstub.GetFunctionAndParameters()
    if function == "initVehicle" {
        return s.initVehicle(APIstub)

    } else if function == "getVehicle" {

        return s.getVehicle(APIstub, args)
    } else if function == "setVehicle" {

        return s.setVehicle(APIstub, args)
    } else if function == "getAllVehicle" {

        return s.getAllVehicle(APIstub)

    fmt.Println("Please check your function : " + function)
    return shim.Error("Unknown function")
}
```

Fig. 4. Example of chaincode

블록체인 네트워크에서 각 사용자와 자동차를 구분할 수 있어야 하고 생성한 데이터의 해시값을 저장할 수 있어야 한다. 따라서 initVehicle 함수를 이용해 초기 자동차 정보를 초기화한다. getVehicle 함수와 setVehicle 함수를 이용해 자동차의 해시값을 저장하고 불러오는 기능을 수행한다. 분산저장소에 데이터의 원본을 성공적으로 저장했을 경우 저장소는 해시값을 출력하며 이 값을 이용해 저장된 데이터를 찾을 수 있다. 따라서 분산저장소에서 생성된 해시값을 저장하는 기능을 수행해야 한다. IPFS에 데이터를 저장하고 해시값을 반환받는 과정은 Fig. 5와 같다.

```
bstudent@bstudentvb:~/go-ipfs$ ipfs daemon
Initializing daemon...
Successfully raised file descriptor limit to 2048.
Swarm listening on /ip4/10.0.2.15/tcp/4001
Swarm listening on /ip4/127.0.0.1/tcp/4001
Swarm listening on /ip4/172.17.0.1/tcp/4001
Swarm listening on /ip4/172.18.0.1/tcp/4001
Swarm listening on /ip6/::1/tcp/4001
Swarm listening on /p2p-circuit/ipfs/QmcW2LJf47GQn7vXK9KgSdjRSgB4bDfoaR
282KdFqeEQC
Swarm announcing /ip4/10.0.2.15/tcp/4001
Swarm announcing /ip4/127.0.0.1/tcp/4001
Swarm announcing /ip4/172.17.0.1/tcp/4001
Swarm announcing /ip4/172.18.0.1/tcp/4001
Swarm announcing /ip6/::1/tcp/4001
API server listening on /ip4/127.0.0.1/tcp/5001
Gateway (readonly) server listening on /ip4/127.0.0.1/tcp/8080
Daemon is ready

문제  출력  디버그 콘솔  터미널  JUPYTER  fabric-node

bstudent@bstudentvb:~$ ipfs add Vehicle.txt
added Qmc3CnB7LV8i9ANUC8gxmeZtQW5E6Xg8rzLQSTPjdQQmvf Vehicle.txt
 27 B / 27 B [=============================================] 100.00%
bstudent@bstudentvb:~$
```

Fig. 5. Example of IPFS

IPFS Daemon을 구동시킨 후 서버에 해당 명령어를 통해 파일의 업로드를 진행하고 업로드가 성공적으로 완료되면 위와 같은 해시값을 출력한다. IPFS의 파일 검색 및 관리를 위해 해시값을 이용한다. 업로드의 결과로 나온 해시값은 체인 코드를 이용해 저장하며 해시값으로 해당 자동차의 데이터를 찾을 수 있다.

4. 분석

자동차의 ECU 데이터는 사용자의 생명과 직결되어 있어 중요성이 매우 크다. 본 장에서는 제안하는 모델의 안전성 및 효율성을 중심으로 분석한다.

4.1 안전성 분석

안전성에 대한 분석은 보안 요구사항에 따라 무결성, 기밀성, 가용성, 내부자 공격, 재전송 공격을 중점으로 분석한다.

4.1.1 무결성

ECU는 자동차의 데이터를 직접 처리하는 장치로서 외부에서 쉽게 접근 및 조작할 수 없어야 한다. 데이터의 변경을 막기 위해 서버에서 발급받은 세션키로 데이터의 해시값을 암호화하여 서버로 전송한 뒤 서버는 차량에서 받은 해시값과 서버가 계산한 해시값을 비교하여 무결성을 검증한다. 무결성 검증이 완료되면 데이터의 해시값은 블록체인에 등록하여 변경이 불가하다.

4.1.2 기밀성

자동차와 서버 사이의 데이터 송·수신 과정에 있어서 공격자가 데이터 도청 및 조작할 수 없도록 하여 기밀성을 보장해야 한다. 자동차와 서버 간의 ECU 데이터의 송·수신 과정은 공개키와 세션키를 사용하여 기밀성을 보장한다.

서버는 자동차 ECU 데이터의 암호화를 위해 세션키를 사용하며 키를 안전하게 전송하기 위해 공개키를 사용한다. 세션키는 자동차의 공개키로 암호화하여 전송하기 때문에 자동차의 개인키로만 복호화가 가능하다. 따라서 공개키 방식을 이용하여 세션키를 전송하기 때문에 키 배송 문제가 해결되며 공격자는 자동차와 서버 간 ECU 데이터의 송·수신 과정에 끼어들어 도청 및 조작이 불가능하다. 특히 세션키는 일회성으로 한 번만 사용하기 때문에 재전송 공격이 불가능하다.

4.1.3 가용성

ECU 데이터를 직접 블록체인에 등록하면 블록체인 메인넷의 부하가 발생할 수 있어 ECU 데이터의 해시값만 등록하고 데이터의 원본은 off-chain인 IPFS에 등록한다. 이때 IPFS의 접근 해시값도 ECU 데이터의 해시값과 같이 블록체인에 등록한다. 블록체인과 IPFS는 분산 시스템으로 누구든지 검증하고 확인할 수 있어야 하며, 네트워크 어느 한 곳에 장애가 발생하여도 가용성을 보장한다.

4.1.4 내부자 공격

중앙집중형식의 시스템과 달리 블록체인은 분산 시스템으로 동일한 데이터를 분산 저장하기 때문에 악의적인 내부 공격자가 내부에서 임의로 데이터를 조작할 수 없다. 원본 ECU 데이터는 IPFS에 분산 저장하고 블록체인에는 ECU 데이터의 해시값, IPFS 접근 해시값을 저장하여 내부 공격자에 의한 조작이 불가능하다.

4.1.5 재전송 공격

서버는 공개키 암호 알고리즘을 이용해 세션키를 안전하게 전송하고, 자동차는 개인키를 이용하여 복호화한다. ECU 데이터의 암호화는 일회성으로 매번 달라지는 세션키를 이용하기 때문에 공격자가 중간에서 키를 탈취하더라도 재전송 공격이 불가하다.

4.2 효율성 분석

ECU 데이터는 대부분 사용자가 스스로 데이터의 조작 여부를 확인할 수 없고, 전문 업체를 통해 확인해야 한다. ECU 데이터를 블록체인과 분산저장소에 저장하면 사용자는 전문 업체를 통해 데이터를 확인할 필요 없이 스스로 확인 및 검증을 할 수 있다. 그리고 지속적인 데이터 수집 및 분석을 통해 자동차 관리 및 판매 등의 분야에서 활용할 수 있다. 수집된 데이터를 이용하면 데이터의 무결성 검증뿐만 아니라 데이터를 활용하여 자동차 정비에 활용할 수 있고 보험 및 자동차 거래 시 중요한 데이터로 사용할 수 있다.

지능형 자동차는 차량이 외부와 통신하며 스스로 주행한다. 이러한 과정에서 ECU는 센서들로부터 데이터를 입력받아 처리하여 차량을 제어하는데 ECU는 데이터를 처리하는 과정에서 지연이 없어야 한다. 데이터 처리에 지연이 발생하여 차량 제어가 늦어지면 큰 사고로 이어질 수 있으므로 ECU는 저 지연 및 신뢰성을 보장해야 한다. 제안하는 시스템에서는 ECU와 서버 간에 암호화된 데이터를 송·수신하기 때문에 ECU의 연산을 요구한다. ECU 데이터의 무결성을 검증하는 기술은 자동차 보안에서 필요한 기술이지만 제안하는 시스템은 ECU 처리장치의 높은 성능을 요구한다. 또한 데이터가 조작되는지 실시간 검증이 불가하고 이후에 확인해야 한다는 단점이 존재한다.

5. 결론

ECU는 자동차의 주행에 관련된 데이터를 처리하여 제어하고 있으며 이는 공격자가 데이터에 대한 공격 및 조작을 통해 탑승자에게 의도적인 상해를 가할 수 있음을 의미한다. 악의적인 사용자에 의해 데이터 조작을 통해 이득을 취하는 사례가 발생하고 있으므로 자동차 데이터 통신에 있어서 신뢰성을 보장해야 하며 데이터가 악의적으로 조작될 수 없도록 안전성을 보장해야 한다.

본 논문에서는 블록체인을 활용하여 ECU 데이터의 무결성을 검증하는 시스템을 제안하였다. 세션키를 이용해 데이터를 암호화하여 통신 과정에서 신뢰성을 보장하며, 해시함수를 사용해 무결성을 검증한다. off-chain인 IPFS에 데이터를 분산 저장하여 가용성을 제공한다. 사용자가 스스로 데이터를 확인할 수 있고 데이터의 해시값은 블록체인에 저장하기 때문에 조작이 불가하다.

향후 연구로는 데이터의 무결성 검증을 실시간으로 가능하도록 시스템을 개선해야 하며, ECU의 연산을 줄일 수 있도록 개선해야 한다.

REFERENCES

[1] S. P. Byeon, T. H. Kang, Chai ting & S. S. Shin. (2022). Integrity Verification of Electronic Control Unit Based on Blockchain. *Proceedings of the Digital Contents Society,* 213-214.

[2] D. G. Lee & S. H. Lee. (2016). Reviews on Connected Car. *Journal of advanced information technology and convergence, 14(1),* 41-45.

[3] M. E. Jung & Y. J. Beom. (2015). Security Threat Trends of the Connected Car. *The Journal of Korean Institute of Communications and Information Sciences,* 83-84.

[4] K. B. Yeon. (2021). Intelligent sensors and artificial intelligence semiconductors for autonomous vehicles. *The Magazine of the IEIE, 48(12),* 43-53.

[5] J. H. Hong & K. H. Lee. (2020). Automotive ECU

Biometric Authentication Using Blockchain. *Journal of the Korea Internet of Things Society, 6(1),* 39-43.

[6] G. M. Lee & J. C. Kim. (2017). Model-based Design and Validation of ADAS on Multicore Environment. *The Korean Society of Automotive Engineers,* 630-633.

[7] G. B. Kang. (2020). A Law and Policy Study on Tuning of Automotive Electronic Control Units (ECU). *Hanyang Law Review, 31(3),* 145-168.

[8] S. S. Lee. (2018), In-Vehicle Network Technologies. *Journal of IKEEE, 22(2),* 518-521.

[9] D. Y. Choi, Y. H. Yoon, J. H. Oh & S. E. Lee. (2019). High-Speed CAN-FD Controller for In-Vehicle Network. *Journal of the Institute of Electronics and Information Engineers, 56(12),* 109-116.

[10] C. Mun. (2019), Status of Standardization for Connected and Automated Driving Vehicles. *Auto Journal, 41(12),* 63-66.

[11] J. W. Mun, H. S. Seo & S. S. Lee. (2018). Research Trends on DSRC and C-V2X Technology. *The Korean Society of Automotive Engineers,* 778-782.

[12] J. S. Kim & Y. S. Choi. Vehicle Communication Technology for Autonomous Driving. Daejeon : IITP.

[13] P. S. Kim. (2017). What is the beginning and end of the Volkswagen Dieselgate?. Global Auto News.

[14] D. J. Lee. (2021). I asked the experts what happens to the diesel truck's urea water manipulation. Autocast.

[15] W. S. Chol. (2020). Trends in Automobile Security Technology in International Conferences. *Journal of the Korea Institute of Information Security & Cryptology, 30(6),* 91-99.

[16] S. H. Kwon & J. H. Lee (2020). Autonomous Vehicle Security Threats and Technology Trends. *Journal of the Korea Institute of Information Security & Cryptology, 30(2),* 31-39.

변 상 필(Sang-Pil Byeon) [정회원]

- 2018년 3월~현재 : 동명대학교 정보보호학과

- 관심분야 : Blockchain, IoT, 정보보안
- E-Mail : byunsp3610@gmail.com

김 호 윤(Ho-Yoon Kim) [정회원]

- 2021년 2월 : 동명대학교 정보보호학과 (공학사)
- 2021년 3월현재 : 동명대학교 컴퓨터미디어공학과 석사과정

- 관심분야 : Blockchain, DID, 암호 프로토콜, IoT
- E-Mail : miask376@gmail.com

신 승 수(Seung-Soo Shin) [정회원]

- 2001년 2월 : 충북대학교 수학과 (이학박사)
- 2004년 8월 : 충북대학교 컴퓨터공학과(공학박사)
- 2005년 3월~현재 : 동명대학교 소프트웨어융합보안학과 교수

- 관심분야 : 암호프로토콜, 네트워크 보안, U-헬스 케어, IoT, 데이터분석
- E-Mail : shinss@tu.ac.kr