Vehicle Data Process System with In-vehicle Blockchain for Mobility Services

Xin XU Tatsuya OKABE Yawen HUANG
Haolun HUANG

The connected smart vehicles and automotive automation leads to new services with user's benefit. As one of examples, Mobility as a Services (MaaS), will take a great share of the automotive market. Generally, these type of the new services are based on data from manufacturing process and/or usage of vehicles. However, the expansion of mobility services will increase the possibility and the temptation for fraud with the purpose of economical benefit. Especially the vehicle data, whose tampering bring high economic profit by low tampering cost, will be targeted with a strong tendency. Although the merit of the connected smart vehicles is often discussed, the security should be severely considered because of the increase of channels to be illegally accessed, i.e. communication unit, data storage and the edge calculation. Furthermore, besides cyber-attacks, the tampering occurs with the owner's consent also disable most existing security solutions. We believe that this type of tampering is severer than the cyber-attacks from outside. As a natural conclusion, a certain measurement to maintain credibility of system security and vehicle data is required. In this paper, we propose a novel on-board vehicle integrated system. It ensures the data reliability of in-vehicle devices, i.e. drive recorders and gateway, which consequently increases the value of vehicles.

Key words :
Blockchain, On-board, Mobility service, Tampering

1. Introduction

The automotive industry has been undergoing a once-in-a-century paradigm shift, i.e. a transition from car ownership to car usage. MaaS will grow most rapidly in the mobility market containing electric vehicles (EV) and autonomous driving vehicles. The MaaS includes smart car dispatching services such as Uber, telematics car insurance, i.e. Pay As You Drive (PAYD) and Pay How You Drive (PHYD), and direct resales of cars between individuals. In the near future, by the spread of EVs, many countries are planning to announce the road tax on EVs instead of gas tax in order to get the budget to repair existing roads and build new ones. Furthermore, from the life cycle assessment (LCA) viewpoint, mandatory installation of actual fuel/battery consumption recording device are regulated, which will be used to evaluate CO_2 emissions. These services are offered based on various types of in-vehicle sensor information and analytical information. Sequentially the risk of unauthorized access and the illegal usage of data will increase with mobility market growth. High reliable information will help produce high-quality services. Besides traditional cyber-attacks, the security and normal operation of the modern vehicle are also exposed to tampering. The purpose of tampering is not to cause specific damages, but to alter the system's behavior in order for the vehicle's owner to gain particular advantages.

Regarding ensuring the reliability of vehicle information, some methods tried to solve the problem by uploading the vehicle data to the cloud and registering the data in blockchain in the cloud[1) 2)]. However, in-vehicle storage should be designed with the following considerations:

1. The communication between vehicles or between a vehicle and the internet is often unstable depending on the locations. This instability results in the difficulty to upload the data to the cloud immediately.

2. In some regions, especially in EU countries, consideration of regulations about direct access to vehicles has begun.

3. Many mobility services are based on real-time vehicle data collection and processing by edge computing.

Many researches or services are taking the embedded database of on-board use. the reduction of data stored in SQLite can improve the lifespan of smart cars, in particular their storage, by minimizing the access[3)]. Previously, unauthorized access to vehicles was mainly intended to steal the safe driving data and personal data. However, the expansion of mobility services will increase the motivation to tamper the in-vehicle data for illegal gain by its users. For example, the mileage and accident record may be tampered with to increase the sales price of used cars, or rough driving history that is disadvantageous for paying insurance premiums might be deleted. an approach was proposed for detecting tampering within modern vehicles by leveraging the advantages of sensitive hashing method[4)]. However, the attacker can use fraud tools to take the root authority by taking advantage of operating system (OS) vulnerabilities. Then, they can tamper with data to replace the hash data and raw data.

In this paper, we propose a secure, real-time, and distributed data storage system with higher fault tolerance and scalability based on blockchain technology. Our proposed system enables the usage of vehicles log in real-time and with high reliability. In addition, digital signature and cryptography hash function are also introduced in our proposed system in order to detect the device spoofing. We implemented our proposed system in a real vehicle and carried out a driving test on a road to prove the feasibility of the system.

2. Technology of In-vehicle Blockchain

2.1 Background of data security in-vehicle

There are three main types of attacks on mobility services: ① attacks on unspecified vehicles by third parties ② attacks on specified vehicles by third parties, and ③ internal crimes by owners and others. Our targeted vehicle data falsification is mainly assumed to be ② and ③ because normal network protection can be exploited against ① .

These specific examples might be tampering with vehicle data by illegally obtaining passwords, taking advantage of vulnerabilities in the OS to masquerade as authentic users and tamper with the data, and tampering with data by using malicious third-party apps. Furthermore, tampering usually takes physical access to the vehicle, as well as making profound changes to the vehicle's hardware. For internal attacks by the owner or others, the possible patterns include physically removing the vehicle storage device to tamper with data, installing a fake electronic control unit (ECU) to tamper with data or programs, and tampering with ECU data via an OBD-II port or wireless communication product. It is extremely difficult to detect the data tampering by vehicle owners or via the physical interface.

Fig. 1 shows one sample of the attack tree to obtain data illegally. To do so, we can show three examples, i.e. the usage of passwords obtained, privilege escalation by exploiting vulnerability of a certain code, and illegal removal of storage and trial to read it on the special device.

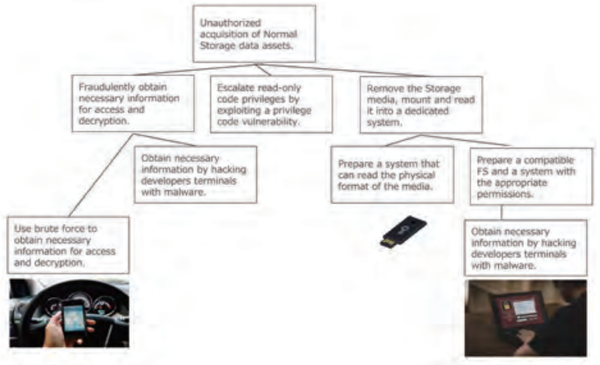

Unauthorized acquisition of Normal Storage data assets.
Fraudulently obtain necessary information for access and decryption.
Escalate read-only code privileges by exploiting a privilege code vulnerability.
Remove the Storage media, mount and read it into a dedicated system.
Obtain necessary information by hacking developers terminals with malware.
Prepare a system that can read the physical format of the media.
Prepare a compatible FS and a system with the appropriate permissions.
Use brute force to obtain necessary information for access and decryption.
Obtain necessary information by hacking developers terminals with malware.

Fig. 1 One sample of attack tree

2.2 The Limitation of Vehicle

Since the communication from the vehicle is not stable and the vehicle data may not be uploaded to the cloud immediately if the network is unstable, the data is also stored locally in the vehicle for a certain period of time. Therefore, tampering countermeasures are needed in the vehicle. Since vehicles are highly cost-sensitive products, it is very important to select proper measures not to increase the manufacturing and the operational costs but to include the anti-tampering capability.

To realize the above, we have to solve three challenges as follows:

1. Frequency of data updates. The vehicle data is updated dynamically in milliseconds depending on the type of sensors.

2. Cost. Since storage volume is limited, the increase of storage for huge amount of data will simply have the impact toward the cost.

3. Lightweight. Since the performance of in-vehicle ECUs is not as good as PC or server, it is extremely crucial to make the in-vehicle software lightweight. Because the ECUs must process other main tasks, only a few percent of CPU power can be allocated to detecting tampering to avoid any impact to main tasks.

2.3 In-vehicle Blockchain

Although the readers of this paper might easily estimate the issues to be solved by the above explanation, we will clearly set the goal of this work as not offering tampered data for services and not uploading it to the service servers. Our basic idea is the usage of blockchain technology which is recently popular as a certain technology to protect the data. Simple usage of the blockchain requests us to prepare the huge computational resources. However, in-vehicle computers are not powerful enough to handle the full blockchain system. Therefore, we extracted basic blockchain mechanisms including distributed ledger and hash technologies, and merged embedded technology to ensure coordination. For this purpose, the new architecture of computer processer, which is often used in a smartphone, will be exploited. In the new architecture, as shown in Fig. 2, there are two types of storages (areas), i.e. normal storage and secure storage. The secure storage is specially designed to store the severe data, ex. password, finger print for login etc. Although the volume of the secure storage is small, we will exploit this storage with an efficient way. The vehicle data, which is input into a vehicle computer, is processed into hash chains and recorded in the local file system (normal storage), and part of the hash chain information is distributedly stored in the secure area of the CPU processor (secure storage). When new data are updated, whether there is a tampering or not can be detected based on the consensus of both areas.

As shown in Table 1, our in-vehicle blockchain technology has advantages over conventional techniques of detecting tampering in in-vehicle applications.

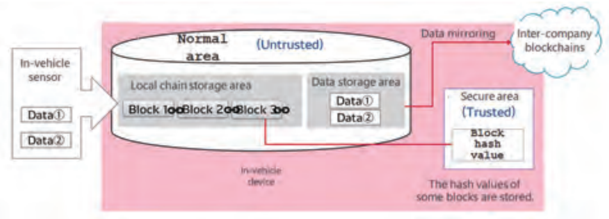
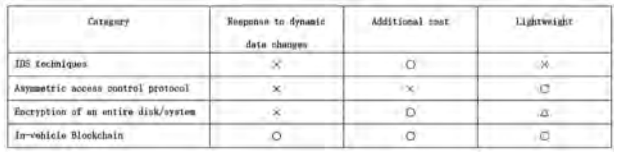


Fig. 2 In-vehicle blockchain architecture

Table 1 Comparison of tamper detection methods



Category	Response to dynamic data changes	Additional cost	Lightweight
IDS techniques	×	○	×
Asymmetric access control protocol	×	×	○
Encryption of an entire disk/system	×	○	△
In-vehicle Blockchain	○	○	○

3. System Design

3.1 System Architecture

The system architecture we developed consists of several operational modules. The example of the modules are as follows:

- Vehicle data analyzer
- Vehicle database
- In-vehicle blockchain
- Cloud-based inter-company blockchain

Fig. 3 shows our developed system which can protect data from vehicle to cloud consistently regardless of communication environment. This system will provide the reliable data by protecting local data in vehicle devices including drive recorders and the smooth data transfer from the vehicle to the cloud with the reduced communication and operational cost by edge processing. The details of the above modules will be explained in the following sections.

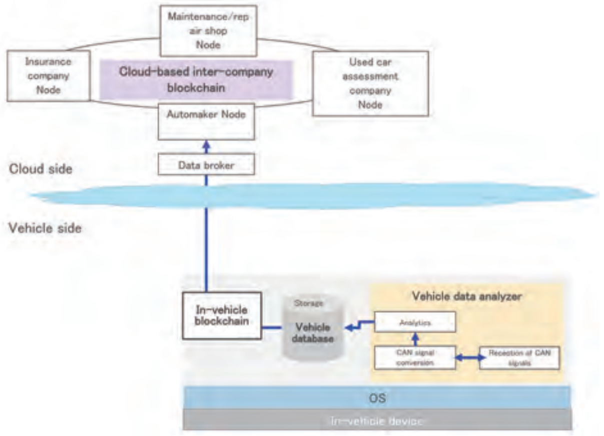


Fig. 3 System architecture

3.2 Vehicle Data Analyzer

The mobility service sometimes requests us to use the data in real time. Some of examples are the usage of speed, acceleration, steering degree, fuel consumption and so on. For LCA service, we have to show the CO_2 emissions by analysis of data based on coming regulations. Furthermore, for used car assessment service, vehicle status and maintenance conditions might be shown in real time. To provide necessary data for these services, we installed the module, so-called vehicle data analyzer, in our system where we can analyze the data in our system.

3.3 Vehicle Database

In our system, we detect data on CAN (controller area network) directly and store them on Mongo DB shortly to avoid user's treatment of data which has possibility to tamper them [5]. To keep the flexibility of data formats, we selected Mongo DB as NoSQL database.

3.4 In-vehicle Blockchain

If we store simply data in Mongo DB, there is possibility to change the data later. Since we want to provide the reliable data to users or service providers, we are protecting the data in Mongo DB by exploiting blockchain technologies. By connecting several data sequentially using hash values, we can protect the data against tampering.

3.5 Cloud-based Inter-company Blockchain

The data from the in-vehicle blockchain will be directly uploaded to cloud-based inter-company blockchain via secured network. This flow will protect the data from the vehicle to the cloud. To access the protected data, we introduced the two concepts of digital signature and cryptography, i.e. hash function, in our proposed system to identify the vehicle client. As a natural way of thinking, the public key of the digital signature will be also registered in the blockchain.

Furthermore, to protect the data, we also newly developed so-called "Multi-layer Chain" as shown in Fig. 4, which can prove non-tampering of vehicle data and recoding of data access. Currently, we are using Hyperledger Fabric (HLF) version 2.2 as the DLT (distributed ledger technology) layer [6].

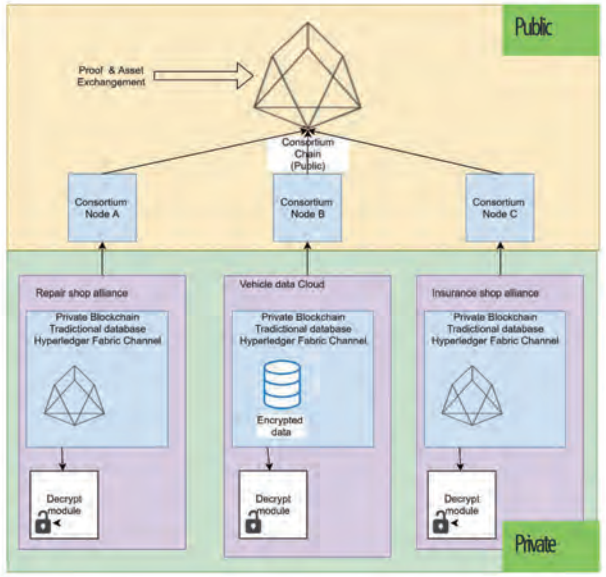


Fig. 4 Multi-Layer Chain

4. System Evaluation

4.1 Evaluation Experiment

We installed our proposed system in a real hybrid vehicle and tested the performance by driving the vehicle around the headquarter of DENSO CORPORATION after finalizing the safety check. We detected CAN data directly by the testing box which connects to the vehicle CAN bus connector. The overall system is shown in Fig. 5. As the testing box, we used Renesas R-Car-H3-Starter Kit [7]. Additionally, to carry out the laboratory test easily, we also install CANoe which can reproduces test data. The real driving test achieved 22 km and 2 hours when we wrote this paper.

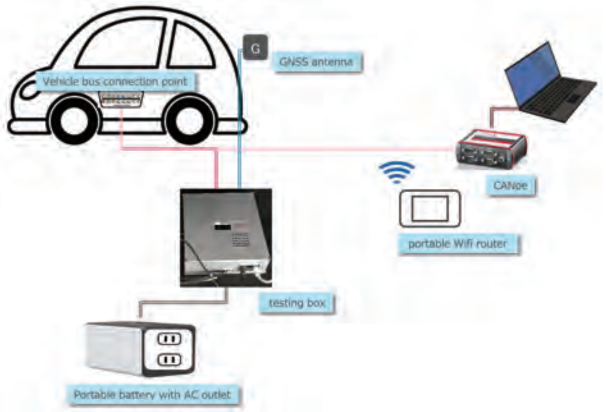


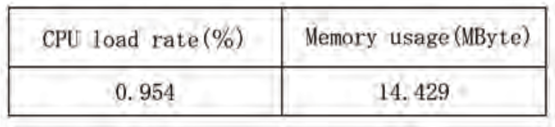
Fig. 5 Vehicle connection for evaluation experiment

4.2 Performance Evaluation

Since we expected that our system will be installed in an existing ECU or an upcoming ECU, the CPU usage and the memory usage should be minimized to avoid any negative impacts to original functionalities of ECU. To confirm the above, we measured the CPU load rate and the memory usage of in-vehicle blockchain. The results were shown in Table 2. In this evaluation, the sampling intervals for CAN bus data collection is 200ms and the ones for checking in-vehicle blockchain data against tampering is 10s.

The Table 2 indicated the average performance value of the driving test. The CPU load rate is only 0.954% and the memory usage is only 14.429 Mbyte. We believe that these results are sufficiently satisfying with our intention, that is any negative impacts to the original functionalities of ECU.

Table 2 Average performance value of the test



CPU load rate(%)	Memory usage(MByte)
0.954	14.429

5. Conclusion

In this paper, we propose a novel on-board vehicle integrated system that can protect vehicle data against tampering. It enhances confidentiality by merging embedded technology with blockchain technologies of hash chain, distributed storage and consensus. A driving test has been also carried out to prove the system feasibility. It provides a solution for secure data distribution among vehicles and companies, with the expectation to increase the value of connected vehicles.

References

1) Chi-Sheng Shih, Wei-Yu Hsieh and Chia-Lung Kao:“Traceability for Vehicular Network Real-Time Messaging Based on Blockchain Technology,” Computer Science, Mathematics,J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.vol. 10, no. 4, pp. 1–21, (2019)

2) Hyoeun Ye and Sejin Park:“Reliable Vehicle Data Storage Using Blockchain and IPFS,” Electronics, 10(1130), 1–15, (2021)

3) Joontaek Oh and Youjip Won:”Embedded DBMS Design forIn-Vehicle Information Management,” Proceedings of the IEEE 7th Non-Volatile Memory Systems and Applications Symposium (NVMSA), pp. 111–112, (2018)

4) Roland Bolboacă, Teri Lenard, Bela Genge and Piroska Haller:“Locality Sensitive Hashing for Tampering Detection in Automotive Systems,” Proceedings of the 15th International Conference on Availability, Reliability and Security, (2020)

5) https://www.mongodb.com/

6) https://www.hyperledger.org/use/fabric

7) https://www2.renesas.cn/us/en/products/automotive-products/automotive-system-chips-socs/r-car-h3-m3-starter-kit

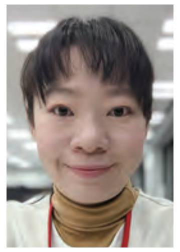
著者

徐 昕
じょ しん

まちづくり企画室 博士（工学）
ブロックチェーン及びトレサビシステム開発
に従事

岡部 達哉
おかべ たつや

まちづくり企画室 博士（工学）
ブロックチェーン及びトレサビシステム開発
に従事



Huang Yawen
ふぁん やうぇん

まちづくり企画室 博士（工学）
ブロックチェーン及びトレサビシステム開発
に従事

黄 浩倫
ふぁん ほるん

まちづくり企画室
ブロックチェーン及びトレサビシステム開発
に従事