Security Assured Vehicle Data Collection Platform by Blockchain: Service Provider's Perspective

Sang-Oun LEE*, Hyunseok JUNG*, Bosuk Han *

**EPIKAR Inc., 06164 #2203 Trade Tower, Yeongdong-daero 511, Gangnam-gu, Seoul, Korea*
Fax: +82 2 6003 0258, Tel: +82 2 466 0621
sangoun.lee@epikar.com, hyunseok.jung@epikar.com, bosuk.han@epikar.com

***Abstract*— The advancements in information and communications technology have connected the disconnected, and changed the daily lives of everybody. The automobile industry is comparatively a laggard to connect its disconnected mobility, but new efforts are introduced to put the car on the network as so called connected cars. A single vehicle contains numerous parts to be assembled just as the numerous types of data which can be collected. Like all the connected things being exposed to a cybersecurity concern, the connected cars are also being exposed to cyber-attacks which can exploit your physical safety from privacy. This research proposes security-assured vehicle data platform through closed blockchain for the service provider who facilitates the data for business. The paper is composed of following. First, the paper identifies the type of data which contains the privacy concerns that can be collected from the vehicle. Second, the authors present how the data collected from the vehicle is valuable to multiple parties. Third, the study reviews why the blockchain is an appropriate technology to collect and redistribute the vehicle collected data. Last, the research proposes a vehicle data platform with a blockchain application which assures confidentiality, integrity and accessibility of the data. The expected contributions of this research are following: First, the research identifies and proposes the value of the vehicle collected data. Second, the study determines and tackles the potential exploits from cyber-attacks to the vehicle data platform. Third, the technical extensions from blockchain to the related industries and potential participants of the platform. The study also expects to extend the technical applications with actual vehicle collected data to closed blockchain.**

***Keywords*— Vehicle data, blockchain, privacy, cybersecurity**

I. INTRODUCTION

The technological progress captured in the Information and communications technology (ICT) sector has introduced new opportunities to other industries. With its variability and adaptability of ICT with other technology, ICT is often coined as a type of general-purpose technology, a term proposed by [1]. Converging with other sectors, ICT has connected all different kinds of things and industries. The automobile is not an exception. Nowadays, more and more vehicles on the road contains more features enhancing driving experience and driver safety by actively adopting the ICT. Furthermore, the data from the vehicles which only collected from the manufacturers are now even more actively spotlighted for other service providers. For instance, the data of vehicle condition from OBD-II devices are now used in the scoring of drivers driving behavior by insurance service providers.

While, because of the data from the vehicle transfers through the network, there is a security concern. If we see any object involving software, in other words, it means hackable. Since 2010, a number of researchers have dedicated to emphasizing the dangers of cyber-attack on vehicles [2]. Furthermore, because the data collected from the vehicles are varied by the driver, the collection of data from a vehicle also contains the privacy concerns. At the same time, because the data collection can contribute to multiple sectors of industries, the data collected from the vehicle it is inevitable regardless of the privacy issues.

The authors then raise questions on the following. What kind of privacy concerns can be found from the vehicle-collected data? How to maintain safety from privacy concerns of the data collected from the vehicle? Which platform will be appropriate to log the data extracted from the vehicle? This paper consists the following approach to answer the posed question above. First, the paper identifies the type of data which contains the privacy concerns that can be collected from the vehicle. Second, the authors present how the data collected from the vehicle are valuable to multiple parties. Third, the study reviews why the blockchain is an appropriate technology to collect the vehicle data. Last, the research proposes a vehicle data platform with a blockchain application which assures confidentiality, integrity and accessibility of the data.

II. PRIVACY-CRITICAL VEHICLE-COLLECTED DATA

From conventional data collected from other type of sensors, vehicle data are grounded by the following distinct characteristics. First, the vehicles are mobile. The mobility of the data has implications for wireless communications as a main medium of data collection. Second, the data can directly have related to the safety-critical applications. Stemmed from mobility feature of the vehicle, because the vehicle is composed of numerous features to operate and assist the driver or passenger, any data that are produced from vehicle may be security-critical. Third, the vehicle data naturally contain privacy of the driver or the passenger. Such data as driving behavior, direction, trip data, fuelling data, and so forth, all data include privacy which can identify the driver [3].

Thus, what is important is that all the data collected from the vehicle will directly or indirectly contains drivers' or passengers' privacy. Privacy is the ability of individuals to decide when, what, and how information about them is disclosed to others [4]. While, the privacy risk is defined as the degree to which an individual believes that a potential for loss is associated with the release of personal information to an entity [5]. For example, the steering data collected from the OBD-II device will not only deliver the information on the steering wheel condition, but also the driving behavior data of the driver when data extracted real-time.

Not only the privacy issue is crucial in maintaining vehicle cybersecurity, other threats are also posed to the vehicles of nowadays. An example of a study in [6] identifies three types of security and privacy concerns from the connected cars based on their review on research related to cybersecurity of the vehicles:

1) Communication threat: malicious attacks (DDoS) to compromise communication
2) Identity management: authentication, authorization, accounting and provisioning of device/user/session
3) Embedded security: all threats of physical and MAC layer

Since the focus of this study is to deliver a proposal for privacy-secured data collection platform, the authors focus on the identity management threat posed on the vehicles.

To readdress the questions posed above, the purpose of the authors engaging in privacy of the data collected from the vehicles suggest that the all the data collected from the vehicle can directly and indirectly related to the privacy concerns. In terms of dealing with such concerns, the crucial task for a data collection platform is to consider how to authenticate, authorize and provide the reliability in order to preserve confidentiality, integrity and accessibility of the data.

III. HOW THE DATA COLLECTED FROM THE VEHICLE IS VALUABLE TO MULTIPLE PARTIES

As modern-day automobiles including electric vehicles are becoming a part of the transportation and mobility industry from all corners of the world and being equipped with several embedded electronic control units (ECUs) networks to support these units, and a host of wired and wireless external interfaces. There exists a great chance to capture an enormous amount of data that can be obtained throughout the whole product life of vehicles [7]. Moreover, it is quite obvious that understanding a car as one of consumer devices is the current trend so that the information collected from modern vehicles such as vehicle lifecycle data may offer excellent potential for further exploitation and additional value creation [8].

However, the automotive industry is still in its embryonic stage of data analytics, which indicates that utilizing the data originated from automobiles for purposes other than driving is not prevalent yet [9]. Also, even a concrete and secure mechanism to promote vehicle data collection platform is not fully available as of today, and from this aspect, the authors assert that establishing the fundamental mechanism for the platform is a matter of the utmost importance. Considering this point, how and what kind of data is obtained from the automobiles should be discussed and identified. It gives rise to the vehicle data platform, reinforced by a blockchain application that ensures a trustworthy data exchange among all involved stakeholders, diminish cybersecurity concerns thanks to its outstanding benefits, namely decentralization and transparency.

To be more specific, this concept is more like a big data pool is formed rather than the information from a single vehicle is gathered one by one and this mechanism is reasonably more efficient given that the sheer number of vehicles running on the road is staggering. Hence, to whom the service is allowed to access, and which sort of data will be shared are determined by smart contracts based on blockchain technology. In a word, security, privacy and standardization concern can be resolved by making use of blockchain technology. Table 1 below presents the overview of data type that would be accumulated in the storage pool. The service providers will inform the drivers which type of the data is required to be transferred and once an agreement between individual vehicle drivers (service consumers) and the service provider is signed, the smart contract will be finalized. The connected vehicles will constantly gather valuable data that will be divided into proper datasets and verified by blockchain technology that it is tamperproof and finally sent encrypted to the cloud [10].

TABLE 1. OVERVIEW OF COLLECTED DATASET

Data column	Example	Possible Business Use
Driver's information	Driver's license ID, driving pattern, accident record, heart rate, patient record	Solutions for insurance and car dealers aiming at individualized services
Vehicle data	Brand, year of manufacture, base weight, emission data	Solutions for Vehicle Management, Driver performance, Maintenance prediction services
Driving data	GPS position, temperature inside, average fuel efficiency	Solutions for OEM
Traffic data	Maximum, minimum and average throughput rate of the road, the frequency of a traffic jam	Reference to urban planning and road traffic policy

The data collection platform is a system exclusively open for the authorized stakeholders categorized into three different entities: i) end users, ii) service providers, and iii) cloud vendor. End users are generally owners of a connected vehicle

who derive benefits from a certain service and will get into contact with the service provider. Superficial value that they can attain would be an incentive to share personal driving data to the providers, yet their driving data can be used to score individual drivers, according to their driving patterns and that information, for instance, can be practically applied to reduce each driver's automobile insurance fee if the driver has a good driving habit. This can even restrain potentially dangerous driving habits among the vehicle drivers and in this way a virtuous circle would be visualized. Besides, end users can be extended to the parties who are not the actual drivers of the connected vehicles but can get help from the collected data when they do pertinent tasks like urban planning, marketing, etc. [11].

The service providers are organizations that generally design the sketch and supply the service for the end users. Raw vehicle lifecycle data aggregated in the cloud will be filtered by the service providers and refined in the standardized form in the system so that, for example, they can anticipate stable revenue sources by providing vehicle fleet management services and automobile maintenance prediction services for the users and the cloud vendor as the facilitator of the infrastructure would be rewarded in return for affording the online storage capacity.

IV. WHY THE BLOCKCHAIN IS AN APPROPRIATE TECHNOLOGY TO COLLECT AND REDISTRIBUTE THE VEHICLE COLLECTED DATA

As mentioned above, data gathered from vehicle-equipped IoT devices are high in scarcity, value in that it can be utilized in diverse ways from services related to automobiles to research and development in vehicles. However, 'current vehicular ecosystem' has not been seeing rapid growth because of the issue about transparency in data utilization that involves data saving, gathering, and the privacy of vehicle owner were remain problematic even in recent days [12]. From this perspective, the importance of blockchain technology is underscored once again since it can assure a reliable data exchange among the involved parties, and moreover bring incentives to the vehicle owners into the data collection platform [13].

The biggest strength of the blockchain technologies is that it can infuse security into the platform thanks to decentralization and transparency [14]. Blockchain technology guarantees a trustworthy data exchange between all involved entities and others. One of the major factors that made it difficult to share or exchange data was how to store personal vehicle data with the transparency while preventing the information from being leaked out. Previously we had no choice but to entirely rely on central authority or intermediaries, which made individuals endure a lot of risk because real control of personal data did not belong to themselves as things stand. In this sense, Blockchain enables transparent management of personal data simultaneously giving full control over the collected information to the end users and service providers chosen by the former, and this will encourage more users to participate in the data collection platform.

Blockchains is merely no more than a series of compiled blocks containing predefined amount of transaction information when they initially showed up as a fundamental technology of Bitcoin about ten years ago [15]. Then, what upgrades this ten-year old technology to be transformed as a state-of-the-art? The answer is a smart contract maintained within Blockchain technology. The vehicle data should be maintained with extra care due to its sensitiveness on security and privacy and it is well known that a cryptographic hash function of blockchain is designed to forestall those problems [13]. Yet, there is no point in paying extra attention if those data are distributed to wrong entities. As a result, the significance of smart contract is emphasized since the application of smart contract would allow the user to choose which service providers can access certain vehicle data for which exploitation purpose. Security of the platform must be treated carefully, and the driver's privacy needs to be respected when designing a vehicle usage data platform, and, as general rule, a service provider should only be allowed to access relevant data collected by a connected vehicle. Once an agreement between the connected vehicle and the service provider is signed, blockchain technology is exploited to (i) verify that the smart contract cannot be tampered with, as well as (ii) make the smart contract available to so called intermediators [16]. Thus, all the participants will not be clueless about the whereabouts of vehicle data in the platform.

Lastly, in order to achieve long-term system build-up, there should be a reasonable inducement for drivers to stay on the platform and that is the gist of the reason why blockchain technology is cut out for our platform model. Vehicle owner's participation is an essential prerequisite for the mechanism; yet, it seems less attractive for individuals providing the information if they receive no reward at current level, thereby the idea of collecting and redistributing the vehicle data may be neglected at the outset. Nevertheless, by implementing the token economy design and the smart contact within the blockchain, the information provider now can be rewarded. Specifically, as soon as automobile data is generated by IoT devices built in vehicle, refined and stored into suitable format on the cloud, the token can be produced as a proof of the data provision for the data owners by approved service providers, which literally becomes a key factor to motivate vehicle owners to spontaneously invest their valuable information into the data collection platform [13].

V. THE PLATFORM PROPOSAL

The authors have identified followings from the previous section of the paper. First, any kind of vehicle-collected data can be privacy-critical. However, the paper also has explored how the vehicle extracted data can be valuable to the multiple parties. Therefore, as a potential service provider utilizing the vehicle data, two major concerns should be addressed in advance of the actual service provision. First, the collected data should be stored in safe, reliable platform which could

assure the confidentiality, integrity and accessibility of the data from privacy infringement. The authors also discovered that the blockchain platform is the appropriate technology to store and use the vehicle-collected data while the privacy protected.

As a service provider, the collected data should be stored and managed with care in order to add values from transactions made from the data platform. In future studies, the authors attempt to propose a vehicle data collection platform (henceforth "Platform") built by closed blockchain technology. The potential contributions of your future proposal are expected as following. First, the Platform will provide safe and reliable transactions of vehicle-collected data demanded by multiple parties. Second, the transparent transactions from the Platform will bring rich value to the data and solutions to every participating actor by solving security and privacy concerns of the data. Third, the Platform will not only contribute to the economic value, but also further value-added on research for developing new models of automobile technology, auto insurance, and so forth.

REFERENCES

[1] Helpman, E. (Ed.). (1998). *General purpose technologies and economic growth*. MIT press.

[2] Yeh, Enoch R., Junil Choi, Nuria G. Prelcic, Chandra R. Bhat, and Robert W. Heath, Jr. "Cybersecurity Challenges and Pathways in the Context of Connected Vehicle Systems." *D-STOP #134*. 2017.

[3] Joy, J., Rabsatt, V., & Gerla, M. (2018). Internet of Vehicles: Enabling safe, secure, and private vehicular crowdsourcing. Internet Technology Letters, 1(1), e16.

[4] Ju, Minho and Mou, Jian, "Privacy as a Commodity Is Not the Case: Privacy Calculus Model for Connected Cars" (2018). WHICEB 2018 Proceedings. 44.

[5] Malhotra, Naresh K., Sung S. Kim, and James Agarwal. "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model." *Information systems research* 15.4 (2004): 336-355.

[6] Ram, P., Markkula, J., Friman, V., & Raz, A. (2018, August). Security and Privacy Concerns in Connected Cars: A Systematic Mapping Study. In *2018 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)* (pp. 124-131). IEEE.

[7] Harnett, K., Harris, B., Chin, D., Watson, G. and (U.S.), J. (2018). *DOE/DHS/DOT Volpe Technical Meeting on Electric Vehicle and Charging Station Cybersecurity Report*. [online] Rosap.ntl.bts.gov.

[8] Swan, M. (2015). Connected Car: Quantified Self becomes Quantified Car. *Journal of Sensor and Actuator Networks, 4*(1), 2-29. doi:10.3390/jsan4010002

[9] Deloitte (2018) Big Data and Analytics in the Automotive Industry. Deloitte Analytics Report.

[10] Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017). BlockChain: A Distributed Solution to Automotive Security and Privacy. *IEEE Communications Magazine, 55*(12), 119-125. doi:10.1109/mcom.2017.1700879

[11] A. Stocker, C. Kaiser, and M. Fellmann, "Quantified Vehicles," *Business & Information Systems Engineering*, vol. 59, no. 2, pp. 125–130, Sep. 2017.

[12] Dorri, A., Kanhere, S., Jurdak, R. and Gauravaram, P. (2017). "Blockchain for IoT security and privacy: The case study of a smart home," *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops).*

[13] Buterin, Vitalik., "A next-generation smart contract and decentralized application platform," Ethereum White Paper, 2014. [Online] Available: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf

[14] Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *2015 IEEE Security and Privacy Workshops*. doi:10.1109/spw.2015.27

[15] Nakamoto, S., "Bitcoin: a peer-to-peer electronic cash system," Whitepaper, 2008. [Online] Available: https://bitcoin.org/bitcoin.pdf

[16] Iansiti, Marco, and Karim R. Lakhani. (January–February 2017) "The Truth about Blockchain." *Harvard Business Review, 95*, 118-127.

Sang-Oun Lee is a graduate student at the University of Chicago Harris School of Public Policy and the Chief Information & Financial Officer at the EPIKAR Inc. Mr. Lee holds bachelor's degree in International Liberal Arts from Waseda University, Tokyo, Japan, and Master of Science degree in Technology Management, Economics and Policy from Seoul National University, Seoul, Korea.
Prior to start his graduate studies at the University of Chicago, Mr. Lee served Assistant Manager at the Korea Internet & Security Agency and The Attached Institute of ETRI for three years specializing in cybersecurity policy research and practice.

Hyunseok JUNG is the Business Development Manager at the EPIKAR Inc. and holds bachelor's degree in International Liberal Arts from Waseda University, Tokyo, Japan.
Mr. Jung was a former Research Assistant at Yuanta Securities. Mr. Jung is currently registered as Certified International Investment Analyst (CIIA®) by the Association of Certified International Investment Analysts (ACIIA).

Bosuk Han is the Chief Executive Officer & Founder at the EPIKAR Inc. Mr. Han holds bachelor's degree in Mechanical Engineering from Hanyang University, Seoul, Korea, and Master of Science degree in Mechanical Engineering from University of Michigan, Ann Arbor, United States.
Mr. Han was a former manager of BMW Group, Korea. Mr. Han was a former member of American Society of Mechanical Engineers (ASME).