Encouraging Data Sharing for Safe Autonomous Driving

Keonhyeong Kim, Im Y. Jung
School of Electronics Engineering
Kyungpook National University
Daegu, South Korea
striker112@knu.ac.kr, iyjung@ee.knu.ac.kr

***Abstract*—More information can be gathered when autonomous or self-driving vehicles can connect to and communicate with other vehicles and their environments, improving safe self-driving. However, we need an effective scheme that encourages drivers to share state information voluntarily while driving because the information can be shared only by their permission. Therefore, this paper proposes an incentive scheme to boost information sharing and hence improve autonomous driving safety.**

Keywords—Autonomous vehicle, Information sharing, Incentive scheme, Integrity, Safe driving

I. INTRODUCTION

Modern vehicles incorporate complex systems to communicate with their environment and other vehicles, and hence enable autonomous driving through sensors and embedded computers [1,2]. Sensor data, i.e., state information, is critical for autonomous vehicles to decide and take various actions without human intervention or assistance. State information from other vehicles or local environment can be shared by interactions among vehicles or between vehicles and environmental sensors. Such as accidents or road conditions can be useful information to enhance self-driving safety [3]. However, information sharing requires permissions from the owner or the vehicle providing the information, and must guarantee information integrity. Therefore, we propose an incentive scheme to encourage information sharing for autonomous vehicles, as well as verifying data integrity.

II. INFORMATION SHARING REWARDS

This section introduces the state information shared among vehicles or between a vehicle and its environment, e.g. dashcam videos of accidents or road conditions; and describes the proposed incentive scheme to share them.

A. Dashcam videos

Although many open APIs [4, 5] provide automotive data, more data local to the vehicle, such as real-time local accident or road conditions, will enhance self-driving safety. This state information can include images or videos representing significant and complex data, for example videos contain information about object shape, shade, location, motion, and interactions with other objects, rather than just discrete digital values. At the images or the videos showing the state at a specific time, a person may get the information, which he/she is interested in, different from other persons.

Dashcams record events around a vehicle in real-time [6]. They have become relatively inexpensive, and hence many drivers have installed them to record accident details to defend themselves. However, recorded videos are generally retained by their owner rather than being shared. Drivers used to buy the dashcams . Dashcams create a series of short video files, and usually erase previous oldest records as required to free ongoing recording capacity [6]. These videos could be helpful to other vehicles if they could be shared in near real-time, e.g. to avoid chain collisions due to a sudden accident, or when an obstacle suddenly appears in the road. Since dashcams record all scenes during driving, detecting and sharing critical scenes without driver interruption could significantly improve autonomous driving safety.

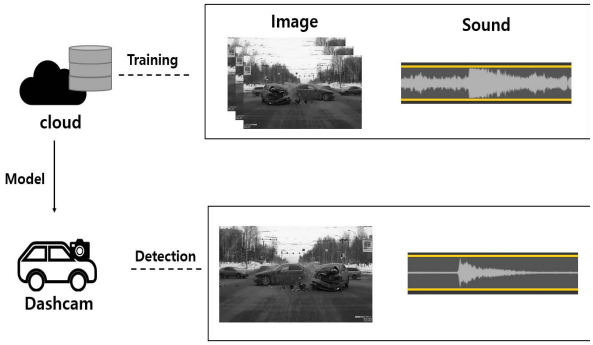

Fig. 1. Our video sharing scheme

We determine the occurrence of an accident from the images and sound of the video recorded by dashcam. The learning model is created in the cloud and stored in the dashcam firmware. The video sharing scheme is described in Fig. 1. Fig. 2 and Fig. 3 show the upload process and the request process of the video with accident scene to be shared [7] each. An accident is detected by dashcam using deep learning and its video is shared based on public blockchain automatically. When a 1 min. video is created, a total of 60 frames are extracted at a rate of one per second for image detection. VGG16 image classification model [8], which was trained on Imagenet [9], was used to detect an accident scene. At the sound classification, the 1 sec recordings were used as the input and features were extracted using Mel Frequency Cepstral Coefficient (MFCC) [10]. The image frames are applied to CNN [11][12] at specific times considering the specifications of the dashcam. The video soundtrack is additionally used to improve detection accuracy.

B. Incentive Scheme

Fig. 4 shows the proposed incentive scheme to share accident video. We adopted Ethereum to implement a public blockchain where all nodes participating in the network can share videos [7]. The incentive the video provider would get was estimated as follows.

- The provider registers its cost, $C_l[v]$, and the time limit t to the blockchain after uploads the video v to the cloud. The k-th requester should propose the

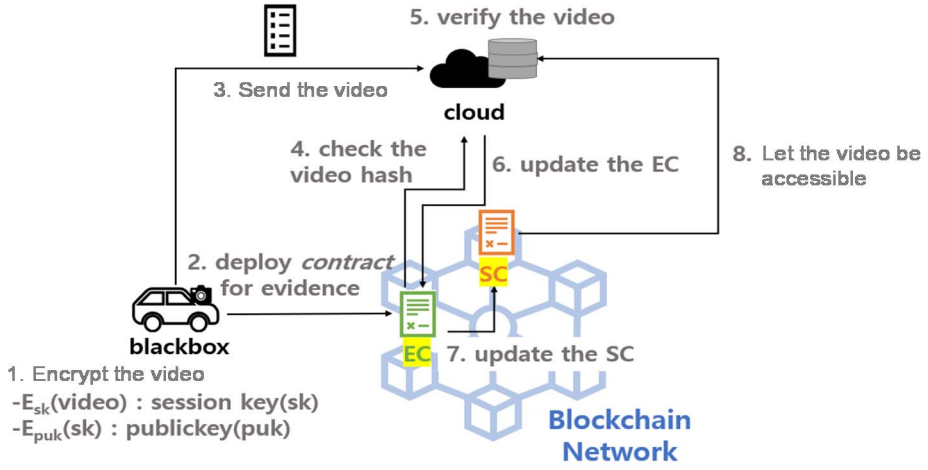

Fig. 2. Video upload

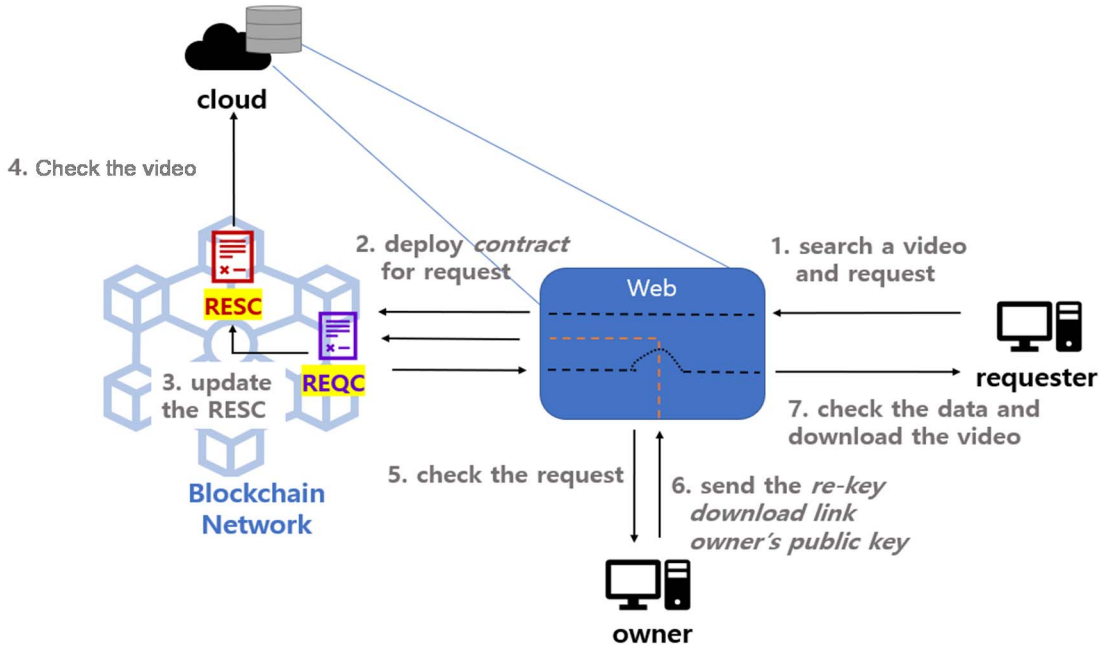

Fig. 3 Video request

reward for the provider, $p_k[v]$, more than $C_k[v]+g$. $C_k[v]$ can be estimated as follows.

$$\begin{cases} C_1[v] = C_U + C_{B_1} + C_N \\ C_k[v] = C_{B_k} \qquad\qquad k > 1 \end{cases}$$

C_U is cloud cost, C_{B_1} and C_{B_k} are blockchain cost, and C_N is communication cost. They are estimated in Table II.

- When the k-th requester downloads the video v, the cost about the video sharing, $C_{k+1}[v]$, is calculated. It includes the cost to use Ethererum blockchain and to communicate in order to manage the video v.
- At t, each requester gets paid back for the remaining after the provider takes its cost and reward; until t, the requester's overpayment is escrowed on the blockchain. Every requester bears the cost and reward for the provider equally.
- At t, let n requesters, the amount to be paid back to the k-th requester is

TABLE II. COST ESTIMATION

	Estimates	Cost Reference
C_U	0.05GB * \$0.023/GB	Amazon S3 [21], 50 MB /Video
C_{B_1} C_{B_k}	\$0.06 \$0.02	Ethereum [22]
C_N	0.924 * 0.05GB * \$12.37/GB	92.4% [23] Mobile Data Communication over Celluar network

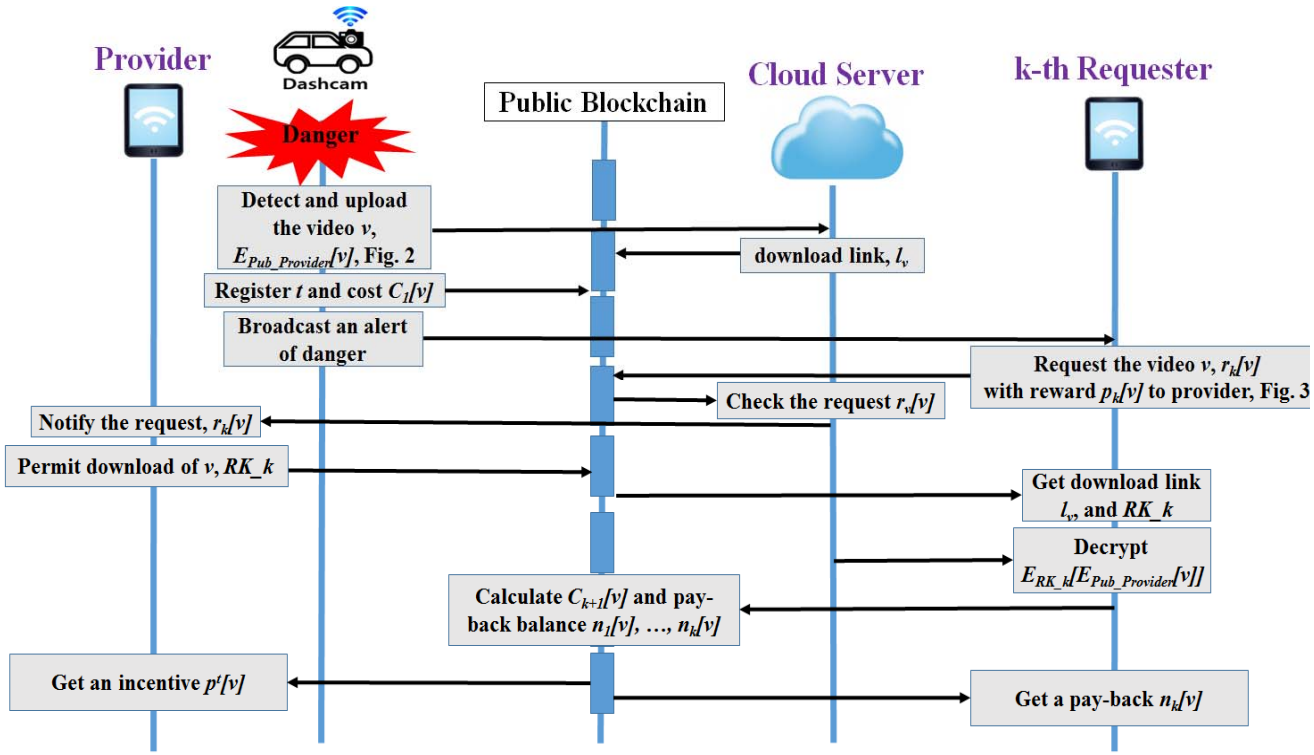

Fig. 4. Proposed incentive scheme for information sharing

TABLE I. SYMBOLS

Symbols	Meaning
$E_{Pub\_Provider}[v]$	Encryption of video v with public key of video provider, *Pub_Provider*
l_v	Download link of video v
$r_k[v]$	Request of video v by k-th requester
t	Time limit to settle incentive and pay-back
$C_k[v]$	Cost of video v paid by k-th requester
$p_k[v]$	Reward for video v provided by k-th requester
g	Minimum reward given to the provider
$p^t[v]$	Reward for video v given to the provider at t, $p^t[v] \geq g$
RK_k	Re-encryption key for k-th requester
$n_k[v]$	Pay-back balance for k-th requester

$$n_k[v] = p_k[v] - \left\{\frac{1}{n}\sum_{i=1}^{n} C_i[v] + g\right\},$$

The provider gets a reward,

$$p^t[v] = n \cdot g + \sum_{i=1}^{n} C_i[v]$$

III. INTEGRITY VERIFICATION AND INCENTIVE ANALYSIS

This section considers video integrity verification and the incentive scheme to encourage data sharing.

A. Integrity Verification

To ensure video integrity, an evidence of these videos is created every minute and sent to the cloud [7]. Time and location details are not transmitted for non-accident videos, whereas the video, time, location, and thumbnail hash for accident cases are shared through the blockchain to ensure video integrity and facilitate retrieval. Four smart contracts were adopted for the blockchain network: the evidence contract (EC) is related to store data from the dashcam as evidence, the search contract (SC) finds the desired video with matching details, and the request (REQC), and response (RESC) contracts apply where the owner transmits a download link and re-encryption key for the video, as shown in Fig. 4 [7].

The EC is a contract regarding the contents of the evidence of the video, which include the owner's account address, hash of the video, the time and location where the accident occurred, the video's thumbnail, and the verification status. When a specific event is detected in the dashcam, this data is created and the EC containing these data is deployed.

The SC is a contract for the video retrieval, which has the EC's address and the time and location information. The SC is deployed from the cloud. When the video is uploaded from the dashcam, the cloud verifies the EC and the SC is updated. The cloud continuously reads the EC data that have been

verified and stores the data in a database.

The REQC is deployed from the requester. It has the requester's public key, the owner's public key, and the download link. When the requester wants to request the original video of the EC, he/she deploys the REQC that has his/her own public key. Then, the address of the REQC and the EC are transmitted to the RESC. The owner can access the REQC to obtain the requester's public key. If the owner wants to share the video, he/she transmits the re-encryption key to the cloud and updates his/her own public key and the download link to the REQC. Because Response contract of the nature of the smart contract, only the owner can send his/her own public key and the link to the REQC. Likewise, only the requester can access the REQC and receive the data.

The RESC deployed from the cloud is used by the owner to determine whether there is a request. When the REQC is deployed, the RESC is updated. The owner always accesses the RESC to check whether there is a request. When the RESC is updated by the REQC, the owner can get the REQC address. Then, the owner can access the REQC to see which video needs to be shared. If he/she wants to share the video, the owner will send the re-encryption key to the cloud and update the REQC by sending the download link and his/her own public key for proxy re-encryption.

The contracts cannot be changed once deployed. The video to be shared is encrypted and stored in cloud, and its hash value verified after decryption.

B. *Incentive Scheme Analysis*

Reward should be provided to the original information provider to encourage data sharing. In addition, the requesters must pay the same cost to download the video such as $\frac{1}{n}\sum_{i=1}^{n} C_i[v] + g$. The more the requestor is, the less the requester pays and the more incentives are given to the provider. Our incentive scheme focuses on fairness between requesters and motivation to share information. The time limit *t* means when the pay-back and the incentive are distributed to the requesters and the provider.

IV. Related Works

Current video sharing methods are based around posting requests and waiting for supplier response(s), which leads to problems to verify data integrity, i.e., video manipulation, and the troublesome process and computational overhead checking for advertisements, and finding and resending the video. Using ViewMap [6], the dashcam creates and uploads view profiles, a compact form of the video, to the cloud for video sharing. However, since the actual video is not uploaded automatically, it is difficult to share the video among vehicles in near real-time. Hossain [13] shared videos from smartphones or cameras around the city to the cloud, using watermarking and authentication to prevent videos from being manipulated in the sharing process or being shared with unwanted people. However, the scheme proposed is not automatic, either.

Blockchain ensures data integrity by distributed node consensus [14, 15]. The data layer checks data authenticity using a digital signature with public key and checks data integrity with a hash function and hash chain of data blocks. Since the blockchain is created and managed by the blockchain node consensus, i.e., without a central control node, it is difficult to modify the blockchain without a majority vote [14]. However, there is no incentive scheme provided by the blockchain, automatic video sharing designed on the blockchain should have its own reward scheme if necessary.

Fraga-Lamas [16] showed many parties can exchange data with each other and communicate via the blockchain. Zhang et al. [17] proposed a P2P file sharing incentive leveraged by cryptocurrency and smart contracts. Free riding and whitewashing can be eliminated by downloading costs, with uploading files earning money. They adopted a game competition model to calculate the appropriate incentive. Shrestha and Vassileva [18, 19] proposed a blockchain based incentive scheme to share user data using P2P-like file sharing with the data provider obtaining an incentive for the data shared. Guo et al. [20] proposed an incentive scheme for competitive organization data sharing. Our scheme provides some incentive to encourage more drivers to share their dashcam videos. However, our incentive scheme does not lead all drivers to compete in order to get the rewards because the accident videos can be obtained around the accident spot at the accident time. Instead, the original video owner can get the reward for sharing his video from the recipients appropriately.

V. Conclusion and Future Works

Modern vehicles commonly incorporate the capacity to share data among vehicles or between the vehicle and environment. Thus, state information local to, but outside the autonomous vehicle, such as accident or road condition video, can be shared and used to enhance self-driving safety. However, such vehicle requires voluntary authorization from the data owner. This paper proposed an incentive scheme to encourage information sharing for autonomous vehicles, while ensuring data verification.

Future study will implement the proposed rewards scheme on an autonomous vehicle prototype, along with the detection scheme for modified copies with the same video content.

Acknowledgment

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Education, Korea (2017R1D1A1B03034950); and the BK21 Plus project funded by the Ministry of Education, Korea (21A20131600011).

References

[1] V. H. Le, J. d. Hartog, and N. Zannone, "Security and Privacy for Innovative Automotive Applications A Survey", *Computer Communications*, 2018, pp. 17-41

[2] S. M. Mahmud, S. Shanker, and I. Hossain, "Secure Software Upload In An Intelligent Vehicle via Wireless Communication Links", in Proc. of *IEEE Intelligent Vehicles Symposium*, 2005, pp. 588-593

[3] S. Park, "Motives and concerns of dashcam video sharing," CHI Conference on Human Factors in Computing Systems, 2016, pp. 4758-4769.

[4] Autonomo, https://otonomo.io/

[5] Hyundai Developers, http://developers.hyundai.com/

[6] M. Kim, J. Lim, H. Yu, K. Kim, Y. Kim, and S. Lee, "ViewMap: Sharing private in-vehicle dashcam videos," in Proc. 14th USENIX Sysp. Netw. Syst. Design Implement. (NSDI), pp. 163-176, 2017

[7] T. Kim, "A Privacy-preserving Dashcam Video Sharing on Blockchain with Automatic Accident Detection," Maser degree thesis, 2019

[8] K. Simonyan and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” CoRR, arXiv:1409.1556 [cs.CV], 2014

[9] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei, “Imagenet: A large-scale hierarchical image database,” in IEEE Conference on Computer Vision and Pattern Recognition, pp. 248–255, 2009

[10] B. Logan, “Mel frequency cepstral coefficients for music modeling,” in Proc. Int. Symp. Music Information Retrieval (ISMIR), 2000.

[11] A. Karpathy, G. Toderici, S. Shetty, T. Leung, R. Sukthankar, and L. Fei-Fei, “Large-scale video classification with convolutional neural networks,” In Proceedings of CVPR, pp. 1725–1732, 2014.

[12] M. Hssayeni, S. Saxena, R. Ptucha, and A. Savakis, “Distracted driver detection: Deep learning vs handcrafted features,” Electronic Imaging, 2017.

[13] M. S. Hossain, G. Muhammad, W. Abdul, B. Song, and B. B. Gupta, “Cloud-assisted secure video transmission and sharing framework for smart cities,” Future Generation Computer Systems, 2017.

[14] W. Gao, W. G. Hatcher, W. Yu, “A Survey of Blockchain: Techniques, Applications, and Challenges,” International Conference on Computer Communication and Networks, 2018, pp. 1-11

[15] S. Dhakal, F. Jaafar, P. Zavarsky, “Private Blockchain Network for IoT Device Firmware Integrity Verification and Update,” IEEE International Symposium on High Assurance Systems Engineering, 2019, pp. 164-170.

[16] P. Fraga-Lamas, T. M. Fernández-Caramés, “A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry,” IEEE Access, vol. 7, 2019, pp. 17578-17598

[17] Q. Zhang, Y. Leng, L. Fan, “Blockchain-based P2P File Sharing Incentive,” IACR Cryptology, 2018

[18] A. K. Shrestha, J. Vassileva, “Blockchain-Based Research Data Sharing Framework for Incentivizing the Data Owners,” ICBC 2018

[19] A. K. Shrestha, J. Vassileva, “User Data Sharing Frameworks: A Blockchain Based Incentive Solution,” IEEE IEMCON 2019

[20] B. Guo et al., “A Secure Incentive Mechanism for Competitive Organization Data Sharing: A Contract Theoretic Approach,”IEEE Access, Vol. 7, pp. 60067 – 60078

[21] https://aws.amazon.com

[22] https://ethgasstation.info

[23] https://www.statista.com/statistics/994889/free-wi-fi-traffic-volumes-in-the-us/, https://www.statista.com/statistics/615419/wireless-data-traffic-in-the-us/