Vehicle data sharing using MPC scheme based on blockchain

Su Jin Shin[1]*, Ye Hyeon Park[1], and Sang Uk Shin[2]

[1] Dept. of Information Security, Pukyong National University, Busan, Republic of Korea
{inuin9014, yhyeon00612}@gmail.com
[2] Div. of Computer Engineering and Artificial Intelligence, College of Information Technology and Convergence, Pukyong National University, Busan, Republic of Korea
shinsu@pknu.ac.kr

Abstract

Data-driven applications are essential to the advancement of many fields, but they often involve data of a sensitive and personal nature. Thus, Privacy-preserving technologies such as MPC (multi-party computation) technology are needed to facilitate a data-driven economy. This paper proposes a privacy-preserving vehicle data sharing system using MPC technology based on blockchain.
Keywords— Blockchain, MPC, FairplayMP, Data Sharing

1 Introduction

Existing vehicle data sharing systems have an interaction step between the data owner and the data requester[2][3]. This may cause problems with personal information protection. Currently, there is a growing interest in and need for systems that can obtain desired data without revealing information about the input values. MPC technology is a technology that jointly performs computations without disclosing the individual inputs of system participants and derives the results desired by participants, making it an excellent technology for protecting personal information. Therefore, this paper proposes a secure vehicle data sharing system in a blockchain environment that adopts FairplayMP[1] technology among MPC technologies.

2 Proposed System

The proposed system applies the FairplayMP technique as an MPC scheme, which is transformed into a blockchain-based system. And, it consists of a data requester, data owner, and blockchain. Figure 1 shows the proposed system, and the operation description of the proposed system is as follows : In the first step, the vehicle data requester deploys a smart contract on the blockchain containing the function for his or her request and the incentives to be provided to the IP(Input Players), RP(Result Players), and CP(Computation Players). In step 2, CP and RP are randomly selected. Afterwards, the IP, which can be seen as the vehicle data owner, garbles its own data and provides garbled input to the CP and RP. In step 3, the received CP computations the Garbled Circuit of the function requested by the data requester and delivers the computationed result to the RP. In step 4, the RP evaluates the Garbled Circuit based on the information delivered to the IP and CP and delivers the value of the Output Circuit to the data requester. The proposed system applied MPC technology to solve the privacy protection

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, Japan, Article No.P-1
*Corresponding author: Dept. of Information Security, Pukyong National University, Busan, 48513, Republic of Korea, Email: inuin9014@gmail.com

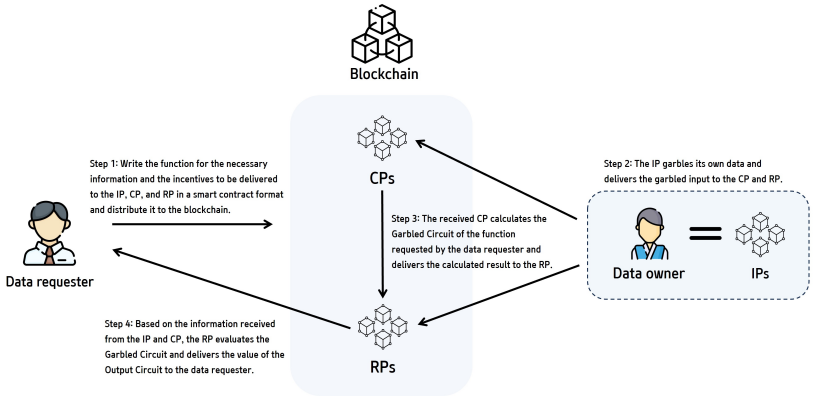

Figure 1: Overview of the Proposed system

problem of system participants. By applying MPC technique that operates in a blockchain environment, it can solve the fairness problem that is difficult to handle in traditional MPC systems. In addition, by sharing only the computed results and not the original data, it provides higher privacy preservation property compared to existing blockchain-based vehicle data sharing schemes. Lastly, the proposed system has the advantage of not using any trusted third party and minimizing the amount of computation of the data provider.

3 Conclusion

In this paper, we proposed a system for securely sharing vehicle data in a blockchain environment by applying FairplayMP. Since the proposed system applies blockchain-based MPC technology, privacy preservation is guaranteed because collaborative computation can be performed and only the computed results are shared without the risk of the original data being leaked or disclosed. In the future, for actual implementation, we plan to continue research to consider and resolve issues such as how to randomly select CP and RP, problems with incentive payments, and punishment when malicious actors participate in the system.

Acknowledgement: This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No.2022R1I1A3063257), and supported by Electronics and Telecommunications Research Institute (ETRI) grant funded by the Korean Government [22ZR1300, Research on Intelligent Cyber Security and Trust Infra].

References

[1] Assaf Ben-David, Noam Nisan, and Benny Pinkas. Fairplaymp: a system for secure multi-party computation. Proceedings of the 15th ACM conference on Computer and communications security, p.257–266, 2008.

[2] Byeong-Gyu eong, Taek-Young Youn, Nam-Su Jho, and Sang Uk Shin. Blockchain-based data sharing and trading model for the connected car. *Sensors*, 20(11):3141, 2020.

[3] Hyoeun Ye and Sejin Park. Reliable vehicle data storage using blockchain and ipfs. *Electronics*, 10(10):1130, 2021.