Auction System Model with Blockchain based MPC Technology

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

[1] Dept. of Information Security, Pukyong National University, Busan, Republic of Korea
{yhyeon00612, inuin9014}@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

In this paper, we investigate an approach that applies Multi-Party Computation (MPC) as a privacy-enhancing technology to protect sensitive and confidential information in the supply auction system. We analyze the auction model using the server-aided MPC technology, and then propse a decentralized auction system using Blockchain-based MPC scheme.

Keywords: Auction System, Multi-Party Computation, Blockchain, Cloud Service

1 Introduction

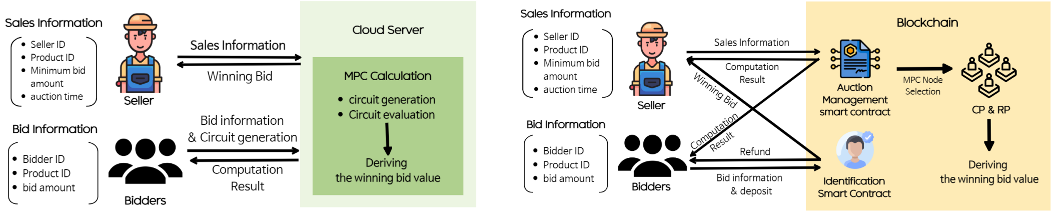
There is a possibility that participants in the auction may engage in dishonest actions such as stealing others' bid information to maximize their profits. To prevent this, MPC that keep inputs private are being applied. In order to reduce the amount of the client's computation, a server-aided MPC technology using cloud servers was presented[1]. When cloud server-aided MPC technology is applied to the auction system, cloud servers are assumed to be semi-honest entities, but they are not trusted entities. And during MPC computation, continuous interaction between servers and clients is required. To address these problems, this paper proposes the privacy-preserving auction system using blockchain-based MPC technology.

2 Auction System using Server-aided MPC

If the server-aided MPC proposed in [1] is applied to the auction system, it is designed as a model consisting of a seller, a server, and bidders as shown in the Figure 1(a). The seller provides sales information, and the bidders provide bid information to the server. The server then provides an MPC computation environment, notifying the computed result(i.e., the winning bid) to both the seller and the bidders. The server performs circuit generation and evaluation the garbled circuit to compute the winning bids of n bidders. After submitting a bid, bidders will still need to interact with the server during the garbled circuit generation and evaluation process. In the auction system, it is desirable that bidders can remain offline after submitting their bids. Furthermore, if a cloud server is compromised, the server is likely to collude with malicious bidders, which leads to a trust issue with the server. Therefore, there are challenges in the practical application of server-aided MPC.

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, Japan, Article No.P-2

*Corresponding author: Dept. of Information Security, Pukyong National University, Busan, 48513, Republic of Korea, Eamil: yhyeon00612@gmail.com



(a) using cloud server-aided MPC

(b) using blockchain based MPC

Figure 1: Auction system

3 Auction system using Blockchain based MPC

We propose a model that applies MPC technology based on blockchain to the auction system, aiming to improve the trust issue related to the cloud server. The proposed model consists of sellers, bidders, and a blockchain, as shown in the Figure 1(b). It manages the auction and verifies identities through smart contracts deployed on the blockchain. The seller posts the sales information on the blockchain, and The bidders send the bid information and the same amount of deposit to identification smart contract. The identification smart contract verifies the bidder's identity and accepts bid information upon authentication. The Auction Management Smart Contract randomly selects MPC computation nodes to compute the winning bid. Assuming this model is based on FairplayMP, the selected nodes act as CP (Computation Players) or RP (Result Players), generating and evaluating circuits[2]. The final evaluation results of the garbled circuit are published on the blockchain. The seller receives the winning bid from the blockchain, and unsuccessful bidders receive a refund of their deposit. Nodes that successfully complete the MPC computation receive incentives, while dishonest nodes are penalized.

4 Conclusion

In this paper, we proposed a model for the privacy-preserving auction system by applying Blockchain-based MPC technology to address the issues that arise when implementing server-aided MPC technology in a cloud environment. As future research, we plan to conduct a comparative analysis of system models based on the type of blockchain and MPC technology, and design specific protocols. We'll also consider issues on incentives and deposits.

Acknowledgement: This research was supported by Korea Institute of Marine Science & Technology Promotion (KIMST) funded by the Ministry of Oceans and Fisheries (201803932), and supported by the MSIT(Ministry of Science and ICT), Korea, under the Special R&D Zone Development Project(R&D) - Development of R&D Innovation Valley support program(2023-DD-RD-0152) supervised by the Innovation Foundation.

References

[1] Yulin Wu, Xuan Wang, Willy Susilo, Guomin Yang, Zoe L Jiang, Siu-Ming Yiu, and Hao Wang. Generic server-aided secure multi-party computation in cloud computing. *Computer Standards & Interfaces*, 79:103552, 2022.

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