

# Combinatorial Resources Auction in Decentralized Edge-Thing Systems Using Blockchain and Differential Privacy

Jianxiong Guo, Xingjian Ding, and Weijia Jia, *Fellow, IEEE*

**Abstract**—With the continuous expansion of Internet of Things (IoT) devices, edge computing mode has emerged in recent years to overcome the shortcomings of traditional cloud computing mode, such as high delay, network congestion, and large resource consumption. Thus, edge-thing systems will replace the classic cloud-thing/cloud-edge-thing systems and become mainstream gradually, where IoT devices can offload their tasks to neighboring edge nodes. A common problem is how to utilize edge computing resources. For the sake of fairness, double auction can be used in the edge-thing system to achieve an effective resource allocation and pricing mechanism. Due to the lack of third-party management agencies and mutual distrust between nodes, in our edge-thing systems, we introduce blockchains to prevent malicious nodes from tampering with transaction records and smart contracts to act as an auctioneer to realize resources auction. Since the auction results stored in this blockchain-based system are transparent, they are threatened with inference attacks. Thus in this paper, we design a differentially private combinatorial double auction mechanism by exploring the exponential mechanism such that maximizing the revenue of edge computing platform, in which each IoT device requests a resource bundle and edge nodes compete with each other to provide resources. It can not only guarantee approximate truthfulness and high revenue, but also ensure privacy security. Through necessary theoretical analysis and numerical simulations, the effectiveness of our proposed mechanisms can be validated.

**Index Terms**—Internet of Things, Blockchain, Smart contract, Edge-thing system, Combinatorial auction, Truthfulness, Revenue, Differential privacy.

## I. INTRODUCTION

WITH the rapid improvement of electronic equipment and communication infrastructure, Internet of Things (IoT) has become a hot research topic connecting the physical environment to the cyberspace system. IoT devices are ubiquitous and play an important role in our lives, such as mobile phones, cameras, automobiles, and traffic sensors. In recent years, the number of IoT devices has exploded. Based on a survey conducted by Cisco [1] [2], they predicted that more than 75 billion IoT devices would go into operation before 2025. These IoT devices produce a large amount of data. How

to utilize these data to better serve the society has attracted more and more attention in academia and industry, and has driven a series of downstream industries such as smart home, smart supply chain, healthcare, and product traceability.

It is not easy to process these data to produce valuable information, which usually involves some artificial intelligence algorithms or data mining techniques. It requires IoT devices to have a certain amount of computing power and storage space. However, most IoT devices are lightweight, which can only temporarily store a small amount of data and perform simple operations. In the traditional cloud-thing system, IoT devices rely on the computing power, network bandwidth, and storage space of cloud centers to implement their own functions. Usually, cloud centers are far away from IoT devices, which leads to high energy consumption and network delay. In addition, it also faces the threat of the single point of failure [3] [4], making this system more unreliable. As a result, the cloud-edge-thing system came into being. There are a lot of edge servers distributed in every corner of the space evenly. These edge nodes provide nearby IoT devices with the resources they need. Thus, IoT devices can offload their tasks to neighboring edge nodes instead of cloud centers. Although it overcomes some defects, especially long distance transmission, in cloud-thing systems, the cloud-edge-thing system does not get rid of the control of cloud centers completely.

Therefore, we focus on the edge-thing system in this paper, which is completely decentralized without the management of a third-party authority. But in the resources allocation between IoT devices and edge nodes, they do not trust each other due to the conflict of interests, in which both entities want to maximize their own revenues. Moreover, the transaction records stored in edge nodes may be maliciously tampered with. With this in mind, blockchain [5] is an opportunity to provide a secure peer-to-peer (P2P) network. Blockchain is a distributed ledger for storing real-time data generated by all active participants in the system. It can not only achieve complete decentralization, but also has the characteristics of tampering-proof and transparency. The secure P2P network proved by blockchain can be used as a supplementary technique to design our edge-thing system.

In order to reflect the real market fluctuation and relationship between supply and demand, auction has been proven to be effective, so that IoT devices can get the resources they need at acceptable prices and edge nodes can benefit from providing resources. In this paper, we design a blockchain-based edge-thing system, where the resources allocation and

J. Guo and W. Jia are with the BNU-UIC Institute of Artificial Intelligence and Future Networks, Beijing Normal University at Zhuhai, Zhuhai, Guangdong 519087, China, and also with the Guangdong Key Lab of AI and Multi-Modal Data Processing, BNU-HKBU United International College, Zhuhai, Guangdong 519087, China. (e-mail: jianxiongguo@bnu.edu.cn; jiawj@uic.edu.cn)

X. Ding are with the School of Software Engineering, Beijing University of Technology, Beijing 100124, China. (e-mail: dxj@bjut.edu.cn)

(Corresponding author: Jianxiong Guo.)

Manuscript received April 19, 2005; revised August 26, 2015.

pricing are realized by a combinatorial double auction mechanism. Here, IoT devices are buyers requesting resources and edge nodes are sellers providing resources. Because we have adopted a completely decentralized architecture, there is no suitable entity to act as an auctioneer responsible for executing the auction mechanism and deciding auction results. In our system, the auction mechanism is stored in the smart contract that is built in the blockchain, which can be run automatically when receiving all requests from IoT devices and edge nodes. Different IoT devices have different requirements for each resource type. For example, a device in smart home needs more computing power to implement intelligent algorithms, but a traffic monitor needs more storage space to store road condition data. Each IoT device usually request a bundle of resources according to its task and gives a total bid, which is the reason for the formulation of a combinatorial double auction. The core of designing an auction mechanism is to ensure the truthfulness, so as to encourage buyers/sellers to bid/ask their true valuations.

Since allocation and pricing results are transparent in the blockchain, it exists possible risk of exposing bids/asks of buyers/sellers. The bidding/asking information is their privacy, which may contain some commercial secrets. Adversaries could infer others' bids/asks through comparing the public auction results in multiple rounds by changing its bid/ask. This is known as "inference attack" [6] [7]. In order to prevent players from being trouble by inference attacks, differential privacy [8] is a promising technology with strong theoretical guarantees that can be introduced in designing auction mechanisms. Even though several differential privacy-based auction mechanisms have been proposed in previous literature [9] [6] [10] [11] [12] [13], they are very different from the auction in our edge-thing systems. First, our auction is combinatorial because every buyer gives a total bid for a bundle of resources. Second, each edge nodes can only provide a limited amount of resource for each resource type. Third, the resource request of an IoT device can only be satisfied by one edge node, and the distance between them is constrained. Consider the real situation in edge-thing systems, we design a differentially private combinatorial double auction mechanism by exploring the exponential mechanism that selects the final pricing with a probability proportional to its corresponding revenue. On the premise of ensuring that the privacy is not exposed, it achieves individual rationality, budget balance, computational efficiency, and expected truthfulness at the same time. Our main contributions can be summarized as follows.

- 1) We propose an novel edge-thing architecture based on blockchain technology to achieve complete decentralization and tempering-proof, in which the built-in smart contract acts as a central coordinator.
- 2) To model a real edge-thing system, we formulate a combinatorial double auction model to achieve resources allocation between IoT devices and edge nodes.
- 3) We introduce the exponential mechanism in differential privacy to our auction model so as to ensure privacy protection, and also achieve the expected truthfulness and approximately high revenue.

- 4) We conduct extensive simulations to evaluate the performances of our proposed mechanisms. The simulation results verify our theoretical analysis.

**Organizations:** In Sec. II, we survey the-state-of-art work. In Sec. III, we introduce the edge-thing system model and define our problem formally. In Sec. IV, we introduce the differential privacy describe the mechanism design in detail. In Sec. V, we give the proofs of related properties. Finally, we evaluate our mechanisms by numerical simulations in Sec. VI and show the conclusions in Sec. VII.

## II. RELATED WORK

In recent years, the related research on resources allocation has attract wide attention in academia. Auction theory has been used in a series of related areas, such as mobile crowdsensing [14] [15] and energy trading [16] [17]. In mobile edge computing environment, Sun *et al.* [18] proposed a double auction mechanism to allocate computing power between IoT devices and edge nodes, where IoT devices can purchase computing power from edge nodes. Habiba *et al.* [19] put forward a reverse auction framework in mobile edge computing based on position, which aimed at maximizing the utility of edge servers. Peng *et al.* [20] designed a multiattribute-based double auction mechanism in vehicular edge computing, where the matching is determined by both price and non-price factors. However, a trusted auctioneer is essential to realize the resources allocation by auction mechanisms, especially for double auction. In P2P distributed edge network, there is no entity suitable acting as an auctioneer that can guarantee the security and reliability.

The emergence of blockchain technology has potentially solved this dilemma. It maintains a decentralized ledger, and can work as the auctioneer by combining smart contracts. Sun *et al.* [21] revised their previous work in [18] by introducing blockchain to achieve a trustworthy platform. Jiao *et al.* [22] proposed an auction-based market model for the allocation of computing resources between miners and edge servers. Ding *et al.* [23] [24] attempted to build a secure blockchain-based IoT system by attracting more IoT devices to purchase computing power from edge servers and participate in the consensus process, where they adopted a multi-leader multi-follower Stackelberg game. Guo *et al.* [25] proposed a secure and efficient charging scheduling system based on DAG-blockchain and double auction mechanism. However, all the transaction models in these works are based on the allocation for a kind of resource. They did not consider the allocation of multiple resources. Moreover, they did not consider the potential risk of privacy disclosure.

Because of the public auction results, the sensitive information of participants is at risk of being exposed. To prevent the adversary from inferring players' sensitive information, Dwork *et al.* [8] founded the theory of differential privacy. McSherry *et al.* [9] first applied the differential privacy to auction mechanism and made a complete theoretical analysis. Chen *et al.* [26] combined the differential privacy with double spectrum auction design in order to maximize social welfare approximately. Guo *et al.* [12] revised their work in [25]

by introducing differential privacy to avoid the leakage of bidding/asking information. Besides, differential privacy has been used in mechanism design of spectrum auction [6] [7], smart grid [27] [28], and mobile crowdsensing [29]. However, applying differential privacy to our combinatorial double auction model is very different from the existing work.

### III. EDGE-THING SYSTEM MODEL

In this section, we introduce the system model of the edge-thing architecture and how to integrate the blockchain as an effective technique to overcome the potential security threats in detail. Here, we consider the time can be discretized into time slots, denoted by  $T = \{t_1, t_2, t_3, \dots\}$ , where each time slot is equal in length. The following discussion is within a time slot, including the combinatorial auction mechanism and consensus process. Finally, the objective function and problem definition can be formulated.

#### A. System Description

In the existing intelligent environment, there are a large number of IoT devices deployed in every corner of our lives, which undertake their own different tasks, such as traffic monitoring, health recording, navigation, and machine learning training. Because of their lightweight nature (limited resources) and delay sensitivity, these IoT devices can attempt to offload their tasks to adjacent edge nodes. In order to quantify the demand for different resources, we assume there are  $k$  kinds of resources in our system, denoted by  $\mathbb{R} = \{r_1, r_2, \dots, r_k\}$ , where each  $r_i \in \mathbb{R}$  represents a certain kind of resource such as computation, memory, storage, or network bandwidth.

A certain number of edge nodes can form an intermediate layer between the more powerful cloud center and mobile IoT devices. In our system, there are  $m$  IoT devices, denoted by  $\mathbb{TD} = \{TD_1, \dots, TD_i, \dots, TD_m\}$ . These IoT devices have limited computing power and storage space, thus not enough to achieve their goals. In order to upgrade the quality of service, the resources that are required by the IoT device  $TD_i$  can be expressed as  $\mathbb{D}_i = \{d_i^1, d_i^2, \dots, d_i^k\}$ , where  $d_i^z \in [d_{min}, d_{max}]$ . Each  $d_i^z \in \mathbb{D}_i$  indicates that IoT device  $TD_i$  requires at least  $d_i^z$  units of the resource  $r_z$ . Similarly, there are  $n$  edge nodes, denoted by  $\mathbb{EN} = \{EN_1, \dots, EN_j, \dots, EN_n\}$ . These edge nodes are responsible for providing different resources to IoT devices. The resources that are provided by the edge node  $EN_j$  can be expressed as  $\mathbb{H}_j = \{h_j^1, h_j^2, \dots, h_j^k\}$ , where  $h_j^z \in [h_{min}, h_{max}]$ . Each  $h_j^z \in \mathbb{H}_j$  indicates that edge node  $EN_j$  provides at most  $h_j^z$  units of the resource  $r_z$ . Therefore, each resource-limited IoT device has to broadcast its resource request to the edge service provider in the hope of getting the resources it wants.

As mentioned earlier, in each time slot, edge nodes make a profit by selling resources and IoT devices complete their tasks by buying resources, which has created a double auction problem. In a double auction model, all players have to submit their requests to the auctioneer. There is an important question about who will assume the role of auctioneer. A natural idea is to let the cloud center be the auctioneer. However, this deviates

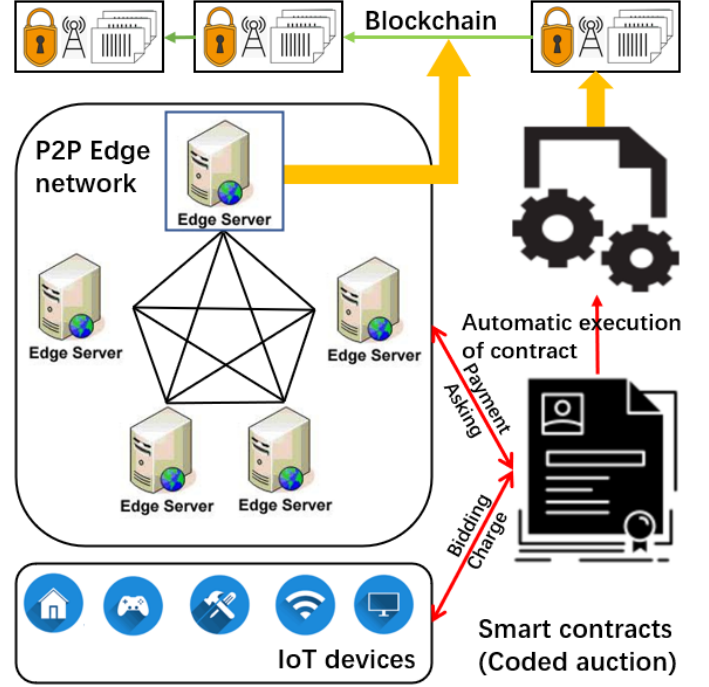


Fig. 1. The architecture of our edge-thing system based on blockchain and smart contract.

from our original intention of getting rid of the cloud centers. There are several potential security threats when trying out a centralized cloud center, which can be summarized as follows.

- 1) **Vulnerability:** the cloud center is attacked or damaged by malicious attackers or unexpected disasters. It will cause the single point of failure.
- 2) **Insecurity:** the bidding/asking information submitted by players could be leaked or tampered with. It will cause data loss and privacy leakage.
- 3) **Unreliability:** the cloud center is biased, and colludes with some nodes for their own benefits. It will cause the auction results to be unfair.
- 4) **Communication security and network delay:** the cloud center is physically far away from IoT devices and edge nodes, which will cause potential security hazards and network delays in the transmission process.

In order to overcome the above drawbacks and achieve the decentralization, the blockchain and smart contract are used as ancillary techniques to prevent tampering and establish a credible system among unfamiliar nodes without the third-party authority. The transaction between IoT devices and edge nodes are stored in the blockchain. Figure 1 exhibits the architecture of our blockchain-enabled edge-thing system. Shown as Figure 1, IoT devices are light nodes that do not store the blockchain but participate in the transaction. Edge nodes are full nodes that store the complete blockchain and perform the consensus process to add new blocks to the blockchain. Moreover, a smart contract is deployed on the blockchain, which plays the role of auctioneer by implementing information interaction between IoT devices and edge nodes, and executing the predefined auction mechanism automatically. Such a system does not rely on a third-party authority to act the auctioneer, and also

inherits the advantages of decentralization, temper resistance, and transparency in the blockchain.

### B. Combinatorial Auction Mechanism

In order to simulate the real situation, we assume that each IoT device submitted its resource request in a bundled way, which formulates a combinatorial auction. For example, an IoT device needs to complete a task of training a deep learning model, thereby it wants to buy computation and memory from edge nodes. It is more reasonable to give a total bid according to its valuation of this task instead of bidding each resource separately. Furthermore, we find that this task can only be accomplished at one edge node. In other words, computing and memory resources must come from the same edge node, which increases the limitation of our model.

In a typical auction, there are three key roles, namely, the buyer, seller, and auctioneer. In our system, IoT devices are buyers, thus buyer set is  $\mathbb{TD}$ ; edge nodes are sellers, thus seller set is  $\mathbb{EN}$ ; and a smart contract is the auctioneer. In each time slot, the buyer requests a set of resources and gives the maximum price it is ready to pay to the edge node for buying these resources. For each buyer  $TD_i \in \mathbb{TD}$ , its bidding information can be denoted by  $\mathcal{B}_i = (\mathbb{D}_i, b_i, dm_i)$  where the  $b_i \in [v_{min}, v_{max}]$  is the total bid (maximum buying price) to buy a bundle of resources  $\mathbb{D}_i$ , and the  $dm_i$  is the maximum tolerant distance from the edge node providing resources to it. For each seller  $EN_j \in \mathbb{EN}$ , its asking information can be denoted by  $\mathcal{A}_j = (\mathbb{H}_j, \mathbf{a}_j)$ , where the  $\mathbf{a}_j = (a_j^1, a_j^2, \dots, a_j^k)$  is the asking vector where each  $a_j^z \in \mathbf{a}_j$  is the unit ask (minimum selling price) per resource  $r_z$ . The bidding information of buyers and asking information of sellers are submitted to the auctioneer, therefore this auction can be defined as

$$\Omega = \left( \{\mathcal{B}_i\}_{TD_i \in \mathbb{TD}}, \{\mathcal{A}_j\}_{EN_j \in \mathbb{EN}} \right). \quad (1)$$

Besides, for each buyer  $TD_i \in \mathbb{TD}$ , its valuation for obtaining the bundle of resources  $\mathbb{D}_i$  is  $v_i \in [v_{min}, v_{max}]$ . For each seller  $EN_j \in \mathbb{EN}$ , it has a cost vector  $\mathbf{c}_j = (c_j^1, c_j^2, \dots, c_j^k)$  where each  $c_j^z \in [c_{min}, c_{max}]$  is the unit cost per resource  $r_z$ .

In each time slot, once collecting the bidding and asking information from players, the auctioneer will determine who are winning buyers and sellers, and how to allocate resources between them. The resource allocation is denoted by a binary matrix  $\mathbf{X}_{m \times n}$ , called "allocation matrix". For each  $x_{ij} \in \mathbf{X}$ ,  $x_{ij} = 1$  if the resources requested by  $TD_i$  are provided by  $EN_j$  according to the result; otherwise  $x_{ij} = 0$ . Besides, the auctioneer needs to determine the clearing price of each resource, which can be denoted by a price vector  $\mathbf{p} = (p_1, p_2, \dots, p_k)$ . For each  $p_z \in \mathbf{p}$ , it is the unit price that buyers have to pay to get a unit of resources  $r_z$ .

**Remark 1.** Here, we have  $c_j^z \in [c_{min}, c_{max}]$  for each resource  $r_z \in \mathbb{R}$  and the price vector  $\mathbf{p} \in [c_{min}, c_{max}]^k$ . For simplicity, we denoted by  $\Theta = [c_{min}, c_{max}]$  in the following description.

### C. Problem Formulation

According to the above definitions, we assume that the utility of each buyer  $TD_i$  is denoted by  $u_i^{TD}$  and the utility

of each seller  $EN_j$  is denoted by  $u_j^{EN}$ . After the auctioneer determines a clearing price vector  $\mathbf{p}$  and its corresponding allocation matrix  $\mathbf{X}$ , the utilities of all losing players are equal to zero. Namely, we have  $u_i^{TD} = 0$  for each losing buyer  $TD_i \in \mathbb{TD}$  if  $\sum_{j=1}^n x_{ij} = 0$  and  $u_j^{EN} = 0$  for each losing seller  $EN_j \in \mathbb{EN}$  if  $\sum_{i=1}^m x_{ij} = 0$ . The utility of each winning buyer is the difference between its valuation and payment toward its requested resources. In summary, for each buyer  $TD_i \in \mathbb{TD}$ , we have

$$u_i^{TD} = v_i - \sum_{j=1}^n x_{ij} \cdot \sum_{z=1}^k p_z \cdot d_i^z. \quad (2)$$

The utility of each winning seller is the difference between the total payment from buyers and total cost. In summary, for each seller  $EN_j \in \mathbb{EN}$ , we have

$$u_j^{EN} = \sum_{z=1}^k (p_z - c_j^z) \cdot \sum_{i=1}^m x_{ij} \cdot d_i^z. \quad (3)$$

Because the requested resources of a buyer must come from the same seller, there is a constraint that  $\sum_{j=1}^n x_{ij} \leq 1$  for each buyer  $TD_i \in \mathbb{TD}$ .

The result of an auction depends on its objective. In this system, we aim at maximizing the revenue of edge computing platform. The corresponding optimization problem can be summarized as to maximize the accumulated utility of all edge nodes, which is shown as the following problem:

$$\max \quad \sum_{j=1}^n \left[ \sum_{z=1}^k (p_z - a_j^z) \cdot \sum_{i=1}^m x_{ij} \cdot d_i^z \right] \quad (4)$$

$$s. t. \quad \sum_{j=1}^n x_{ij} \leq 1, \forall TD_i \in \mathbb{TD} \quad (4a)$$

$$\sum_{i=1}^m x_{ij} \cdot d_i^z \leq h_j^z, \forall r_z \in \mathbb{R}, \forall EN_j \in \mathbb{EN} \quad (4b)$$

$$\sum_{j=1}^n x_{ij} \cdot \delta_{ij} \leq dm_i, \forall TD_i \in \mathbb{TD} \quad (4c)$$

$$x_{ij} \in \{0, 1\}, \forall TD_i \in \mathbb{TD}, \forall EN_j \in \mathbb{EN}. \quad (4d)$$

where  $\delta_{ij}$  is the transmission distance between buyer  $TD_i$  and seller  $EN_j$ . Constraint (4a) represents the many-to-one relationship from IoT devices to an edge node. Constraint (4b) states that the total consumption of each kind of resource  $r_z$  cannot be larger than the maximum amount  $h_j^z$  that can be provided by an edge node  $EN_j$ . Constraint (4c) implies that the distance between an IoT device  $TD_i$  and the edge node that provides it with resources cannot be larger than the maximum distance allowed by this IoT device. This optimization problem can be classified as an integer linear programming problem, thus it is NP-hard.

## IV. MECHANISM DESIGN

In this section, we first introduce basic principles of designing an effective combinatorial auction mechanism. Due to the use of blockchain technology, the transactions in this system become transparent. That is to say, all auction

results, including winners and clearing price, will be made public, which makes the system face the threat of inference attack. Therefore, we introduce the differential privacy into our mechanism design to avoid accidental disclosure of users' bidding/asking information.

### A. Design Rationales

An effective auction mechanism has to satisfy the following four properties: individual rationality, budget balance, computational efficiency, and truthfulness.

**Definition 1** (Individual Rationality). *An auction is individually rational if and only if the utilities of all players are non-negative. In our auction  $\Omega$ , we have  $u_i^{TD} \geq 0$  for each buyer  $TD_i \in \mathbb{TD}$  and  $u_j^{EN} \geq 0$  for each seller  $TN_j \in \mathbb{TN}$ , where  $u_i^{TD}$  and  $u_j^{EN}$  are defined in (2) and (3).*

**Definition 2** (Budget Balance). *An auction is budget balanced if and only if the auctioneer is profitable. In our auction  $\Omega$ , that is*

$$\sum_{j=1}^n \left[ \sum_{z=1}^k (p_z - a_j^z) \cdot \sum_{i=1}^m x_{ij} \cdot d_i^z \right] \geq 0. \quad (5)$$

**Definition 3** (Computational Efficiency). *The auction result can be obtained in polynomial time.*

In an auction, players could manipulate their bids/asks in a strategical sense in order to win the auction. The truthfulness is a concept that encourages players in an auction to bid/ask according to their valuations/costs strictly. However in some cases, it is difficult to reach an exact truthfulness. Thus, we can consider an approximate truthfulness instead, called  $\gamma$ -truthfulness [30], which ensures there is no one gaining more than  $\gamma$  utility when bidding/asking truthfully.

**Definition 4** ( $\gamma$ -truthfulness). *An auction is approximately truthful if and only if each player bids/asks truthfully is approximate to one of its dominant strategies. In our auction  $\Omega$ , for each buyer  $TD_i \in \mathbb{TD}$ , we have*

$$\mathbb{E} [u_i^{TD}(v_i, \Omega_{-i})] \geq \mathbb{E} [u_i^{TD}(b_i, \Omega_{-i})] - \gamma \quad (6)$$

where  $\Omega_{-i}$  is other players' strategies except  $TD_i$ . For each seller  $EN_j \in \mathbb{EN}$ , we have

$$\mathbb{E} [u_j^{EN}(c_j, \Omega_{-j})] \geq \mathbb{E} [u_j^{EN}(a_j, \Omega_{-j})] - \gamma \quad (7)$$

where  $\Omega_{-j}$  is other players' strategies except  $EN_j$ .

When we discuss the truthfulness in our auction, we assume that the requested bundle  $\mathbb{D}_i$  submitted by the buyer and the total resources  $\mathbb{H}_j$  submitted by the seller are all believable because they can be monitored. Due to the truthfulness, no player is motivated to manipulate its strategy to gain more utility, which makes the strategic decision of players easier and guarantees a fair competitive environment.

### B. Differential Privacy

The blockchain applied in our system can only ensure the security at the physical level, but it cannot prevent inference attacks. A curious player can infer other players' strategies

by changing its own bid/ask in continuous auction rounds and analyzing the relevant auction results. With the help of other players' strategies, the attacker is able to make decisions in their favor and increase its benefits, thus undermining the fairness. To prevent this kind of threat, we choose to design a differentially private auction mechanism. Differential privacy is a technique that makes the attacker not distinguish between two neighboring inputs with high probability [8]. Two datasets,  $\mathbf{s} = (s_1, s_2, \dots, s_i, \dots)$  and  $\mathbf{s}' = (s_1, s_2, \dots, s'_i, \dots)$ , are neighboring if and only if they have exactly one different element. For convenience, we denote by the bids of all buyers  $\mathbf{b} = (b_1, b_2, \dots, b_m)$  and the asks of all sellers  $\mathbf{A} = (a_1, a_2, \dots, a_n)$ . The definition of differential privacy is shown as follows.

**Definition 5** (Differential Privacy). *We simplify our auction mechanism as a function  $M(\cdot)$  that maps input bids  $\mathbf{b}$  and input asks  $\mathbf{A}$  to a clearing price  $\mathbf{p}$ . The mechanism  $M(\cdot)$  gives  $\epsilon$ -differential privacy if and only if, for any two neighboring inputs  $(\mathbf{b}, \mathbf{A})$  and  $\{(\mathbf{b}', \mathbf{A}) \text{ or } (\mathbf{b}, \mathbf{A}')\}$ , we have*

$$\Pr[M(\mathbf{b}, \mathbf{A}) = \mathbf{p}] \leq \exp(\epsilon) \cdot \Pr[(M(\mathbf{b}', \mathbf{A}) = \mathbf{p})] \quad (8)$$

$$\Pr[M(\mathbf{b}, \mathbf{A}) = \mathbf{p}] \leq \exp(\epsilon) \cdot \Pr[(M(\mathbf{b}, \mathbf{A}') = \mathbf{p})] \quad (9)$$

where the constant  $\epsilon$  is privacy budget.

The privacy budget is a parameter for controlling the degree of privacy protection that a mechanism gives. Generally speaking, the smaller the privacy budget, the stronger the privacy protection. By introducing the differential privacy into our auction mechanism, the change of a player's bid/ask will not significantly affect the final clearing price. Thus, it prevents us from inference attacks through manipulating strategies and analyzing auction results.

Exponential mechanism [8] is one of the mainstream methods to realize practical differential privacy. It depends on an "score" function  $Q(\cdot)$  that maps input/output pairs to scores. The score function in our auction can be defined as  $Q((\mathbf{b}, \mathbf{A}), \mathbf{p})$ , where a candidate output is more likely to be chosen if its score is higher. Thus, the exponential mechanism can be defined as follows.

**Definition 6** (Exponential Mechanism). *Given an output  $\mathbf{p} \in \Theta^k$ , a score function  $Q(\cdot)$ , and a privacy budget  $\epsilon$ , the exponential mechanism  $M(\mathbf{b}, \mathbf{A})$  selects  $\mathbf{p}$  as its output with a probability that is proportional to its score  $\epsilon Q((\mathbf{b}, \mathbf{A}), \mathbf{p})$ . Thus, we have*

$$\Pr[M(\mathbf{b}, \mathbf{A}) = \mathbf{p}] \propto \exp \left( \frac{\epsilon Q((\mathbf{b}, \mathbf{A}), \mathbf{p})}{2\Delta Q} \right) \quad (10)$$

where  $\Delta Q$  is the sensitivity of score function  $Q(\cdot)$ . That is the largest difference of their scores for any two neighboring inputs  $(\mathbf{b}, \mathbf{A})$  and  $\{(\mathbf{b}', \mathbf{A}) \text{ or } (\mathbf{b}, \mathbf{A}')\}$ , which can be denoted by  $\Delta Q = \max_{\mathbf{p}} \max_{(\mathbf{b}, \mathbf{A}), (\mathbf{b}', \mathbf{A}')} \{ |Q((\mathbf{b}, \mathbf{A}), \mathbf{p}) - Q((\mathbf{b}', \mathbf{A}), \mathbf{p})|, |Q((\mathbf{b}, \mathbf{A}), \mathbf{p}) - Q((\mathbf{b}, \mathbf{A}'), \mathbf{p})| \}$ .

### C. Algorithm Design and Description

The design goal of our auction mechanism is to maximize the revenue of edge computing platform approximately, but

**Algorithm 1** DPAM

---

**Input:**  $(\{\mathcal{B}_i\}_{TD_i \in \mathbb{TD}}, \{\mathcal{A}_j\}_{EN_j \in \mathbb{EN}}), \varepsilon, \Theta$   
**Output:**  $\mathbf{X}_p, p$

```

1: Initialize  $\Delta R = \sum_{j=1}^n (c_{max} - c_{min}) \cdot \sum_{z=1}^k h_j^z$ 
2: for each  $p \in \Theta^k$  do
3:   // Winning candidate determination
4:   Initialize  $x_{ij} = 0$  for each  $x_{ij} \in \mathbf{X}_p$ 
5:   Initialize  $\mathbb{TD}_c \leftarrow \emptyset$ 
6:   for each  $TD_i \in \mathbb{TD}$  do
7:     if  $\sum_{z=1}^k p_z \cdot d_i^z \leq b_i$  then
8:        $\mathbb{TD}_c \leftarrow \mathbb{TD}_c \cup \{TD_i\}$ 
9:     end if
10:  end for
11:  Sort the  $\mathbb{TD}_c$  s.t.  $\sum_{z=1}^k d_1^z \geq \sum_{z=1}^k d_2^z \geq \dots$ 
12:  // Assignment
13:  Initialize  $\{h_j^{1'}, h_j^{2'}, \dots, h_j^{k'}\}$  where  $h_j^{z'} = h_j^z \in \mathbb{H}_j$ 
14:  for each  $TD_i \in \mathbb{TD}_c$  do
15:    Initialize  $\mathbb{EN}_{c,i} \leftarrow \emptyset$ 
16:    for each  $EN_j \in \mathbb{EN}$  do
17:      if  $h_j^{z'} \geq d_i^z$  for each  $r_z \in \mathbb{R}$ ,  $\delta_{ij} \leq dm_i$ , and
         $\sum_{z=1}^k (p_z - a_j^z) \cdot d_i^z \geq 0$  then
18:         $\mathbb{EN}_{c,i} \leftarrow \mathbb{EN}_{c,i} \cup \{EN_j\}$ 
19:      end if
20:    end for
21:    if  $\mathbb{EN}_{c,i} \neq \emptyset$  then
22:       $EN_{j^*} \leftarrow \arg \min_{EN_j \in \mathbb{EN}_{c,i}} \{\delta_{ij}\}$ 
23:      for each  $r_z \in \mathbb{R}$  do
24:         $h_{j^*}^{z'} \leftarrow h_{j^*}^{z'} - d_i^z$ 
25:      end for
26:       $x_{ij^*} \leftarrow 1$ 
27:    end if
28:  end for
29:   $R((b, A), p) = \sum_{j=1}^n [\sum_{z=1}^k (p_z - a_j^z) \sum_{i=1}^m x_{ij} d_i^z]$ 
30: end for
31: // Pricing
32: Select a  $p \in \Theta^k$  according to the selection distribution:
    
$$\Pr[M(b, A) = p] = \frac{\exp\left(\frac{\varepsilon R((b, A), p)}{2\Delta R}\right)}{\sum_{p' \in \Theta^k} \exp\left(\frac{\varepsilon R((b, A), p')}{2\Delta R}\right)}$$

33: return  $\mathbf{X}_p, p$ 

```

---

achieve  $\varepsilon$ -differential privacy,  $\gamma$ -truthfulness, individual rationality, budget balance, and computational efficiency at the same time. The mechanism can be divided into three stages, winning candidate determination, assignment, and pricing. The procedure is shown in Algorithm 1.

In the winning candidate determination, we first select a subset of  $\mathbb{TD}$  as winning buyer candidates, which is denoted by  $\mathbb{TD}_c \subseteq \mathbb{TD}$ . Given a price vector  $p \in \Theta^k$ , we have  $TD_i \in \mathbb{TD}_c$  if and only if it satisfies

$$\sum_{z=1}^k p_z \cdot d_i^z \leq b_i. \quad (11)$$

Then, we sort the set of winning buyer candidates  $\mathbb{TD}_c$  in a descending order according to their amount of requested resources. For each buyer  $TD_i \in \mathbb{TD}_c$ , its amount of requested resources is defined as  $\sum_{z=1}^k d_i^z$ . Thus, we sort  $\mathbb{TD}_c =$

$\{TD_1, TD_2, \dots\}$  where they satisfy  $\sum_{z=1}^k d_1^z \geq \sum_{z=1}^k d_2^z \geq \dots$  definitely. Next, for each buyer  $TD_i \in \mathbb{TD}_c$ , we need to determine its winning seller candidates, which is denoted by  $\mathbb{EN}_{c,i} \in \mathbb{EN}$ . We have  $EN_j \in \mathbb{EN}_{c,i}$  if and only if it satisfies three conditions.

- 1) Its remaining resources  $\mathbb{H}_j'$  are sufficient. In other words, we have  $h_j^{z'} \geq d_i^z$  for each  $r_z \in \mathbb{R}$ .
- 2) Its distance from  $TD_i$  is close enough. Thus, we have  $\delta_{ij} \leq dm_i$ .
- 3) It is profitable by providing resources to buyer  $TD_i$ . Here, we have  $\sum_{z=1}^k (p_z - a_j^z) \cdot d_i^z \geq 0$ .

Condition (1) and (2) is obvious. If Condition (3) cannot be satisfied, providing resources for  $TD_i$  by  $EN_j$  ( $x_{ij} = 1$ ) will lead to a decrease in the objective value.

Given a buyer  $TD_i \in \mathbb{TD}_c$ , we can get its winning seller candidates  $\mathbb{EN}_{c,i}$ . If  $|\mathbb{EN}_{c,i}| \geq 1$ , how can we select the best one to provide resources? In the assignment stage, we can think about it in two directions. The first strategy is to consider load balancing, and we try our best to arrange the edge node with more idle resources to provide service. The second strategy is to consider saving network bandwidth, and we try our best to arrange the edge node that is closest to the target buyer  $TD_i$ . Because an edge node can provide a variety of resources, how to quantify "idle resources" is difficult. Thus, we use the second strategy here, where we select an  $EN_{j^*} \in \mathbb{EN}_{c,i}$  that satisfies

$$EN_{j^*} = \arg \min_{EN_j \in \mathbb{EN}_{c,i}} \{\delta_{ij}\} \quad (12)$$

to provide resources to the buyer  $TD_i$ .

From the above process, we can obtain winning buyers and winning sellers, and their corresponding allocation matrix  $\mathbf{X}$  given a price vector  $p$ . The next pricing stage is to determine which price vector  $p \in \Theta^k$  we select. This pricing process comes from both the uniform pricing [31] and the exponential mechanism. Given a price vector  $p$ , it generates an allocation matrix  $\mathbf{X}_p$ , then we can calculate the corresponding revenue of the platform as (4), denoted by

$$R((b, A), p) = \sum_{j=1}^n \left[ \sum_{z=1}^k (p_z - a_j^z) \cdot \sum_{i=1}^m x_{ij} \cdot d_i^z \right]. \quad (13)$$

We make this platform revenue as the score of price  $p$ . The sensitivity of score function  $R(\cdot)$  can be formulated as

$$\Delta R = \sum_{j=1}^n (c_{max} - c_{min}) \cdot \sum_{z=1}^k h_j^z \quad (14)$$

since  $p_z - a_j^z \leq c_{max} - c_{min}$  and  $\sum_{i=1}^m x_{ij} \cdot d_i^z \leq h_j^z$ . Then, we repeat the above process to calculate platform revenues under all possible price  $p \in \Theta^k$ . To determine the final pricing, we define the probability distribution of price vectors as follows.

$$\Pr[M(b, A) = p] = \frac{\exp\left(\frac{\varepsilon R((b, A), p)}{2\Delta R}\right)}{\sum_{p' \in \Theta^k} \exp\left(\frac{\varepsilon R((b, A), p')}{2\Delta R}\right)} \quad (15)$$

where  $R((b, A), p)$  is defined in (13) and  $\Delta R$  is defined in (14). Given all possible price  $p \in \Theta^k$  and their scores, in

the pricing stage, it randomly select a price vector  $\mathbf{p}$  with the probability  $\Pr[M(\mathbf{b}, \mathbf{A}) = \mathbf{p}]$  shown as (15).

## V. THEORETICAL ANALYSIS

In this section, we describe the theoretical analysis of how our proposed mechanism DPAM, shown as Algorithm 1 satisfies desirable properties.

**Theorem 1.** *The DPAM achieves  $\varepsilon$ -differential privacy.*

*Proof.* Given two neighboring inputs  $(\mathbf{b}, \mathbf{A})$  and  $(\mathbf{b}', \mathbf{A})$ , the mechanism  $M$  randomly select a clearing price  $\mathbf{p}$  from  $\Theta^k$ . Thus, the probability ratio of their corresponding probability selected by the  $M$  is shown as follows.

$$\begin{aligned} & \frac{\Pr[M(\mathbf{b}, \mathbf{A}) = \mathbf{p}]}{\Pr[M(\mathbf{b}', \mathbf{A}) = \mathbf{p}]} \\ &= \frac{\exp\left(\frac{\varepsilon R((\mathbf{b}, \mathbf{A}), \mathbf{p})}{2\Delta R}\right)}{\sum_{\mathbf{p}' \in \Theta^k} \exp\left(\frac{\varepsilon R((\mathbf{b}, \mathbf{A}), \mathbf{p}')}{2\Delta R}\right)} \cdot \frac{\exp\left(\frac{\varepsilon R((\mathbf{b}', \mathbf{A}), \mathbf{p})}{2\Delta R}\right)}{\sum_{\mathbf{p}' \in \Theta^k} \exp\left(\frac{\varepsilon R((\mathbf{b}', \mathbf{A}), \mathbf{p}')}{2\Delta R}\right)} \\ &= \exp\left(\frac{\varepsilon[R((\mathbf{b}, \mathbf{A}), \mathbf{p}) - R((\mathbf{b}', \mathbf{A}), \mathbf{p})]}{2\Delta R}\right) \cdot \frac{\sum_{\mathbf{p}' \in \Theta^k} \exp\left(\frac{\varepsilon R((\mathbf{b}', \mathbf{A}), \mathbf{p}')}{2\Delta R}\right)}{\sum_{\mathbf{p}' \in \Theta^k} \exp\left(\frac{\varepsilon R((\mathbf{b}, \mathbf{A}), \mathbf{p}')}{2\Delta R}\right)} \\ &\leq \exp\left(\frac{\varepsilon}{2}\right) \cdot \frac{\sum_{\mathbf{p}' \in \Theta^k} \exp\left(\frac{\varepsilon[R((\mathbf{b}, \mathbf{A}), \mathbf{p}') + \Delta R]}{2\Delta R}\right)}{\sum_{\mathbf{p}' \in \Theta^k} \exp\left(\frac{\varepsilon R((\mathbf{b}, \mathbf{A}), \mathbf{p}')}{2\Delta R}\right)} \\ &\leq \exp\left(\frac{\varepsilon}{2}\right) \cdot \exp\left(\frac{\varepsilon}{2}\right) \cdot \frac{\sum_{\mathbf{p}' \in \Theta^k} \exp\left(\frac{\varepsilon R((\mathbf{b}, \mathbf{A}), \mathbf{p}')}{2\Delta R}\right)}{\sum_{\mathbf{p}' \in \Theta^k} \exp\left(\frac{\varepsilon R((\mathbf{b}, \mathbf{A}), \mathbf{p}')}{2\Delta R}\right)} \\ &= \exp(\varepsilon). \end{aligned}$$

By symmetry, we have  $\Pr[M(\mathbf{b}, \mathbf{A}) = \mathbf{p}] / \Pr[M(\mathbf{b}', \mathbf{A}) = \mathbf{p}] \geq \exp(-\varepsilon)$ . According to Definition 5, the DPAM is  $\varepsilon$ -differentially private to buyers.

Given two neighboring inputs  $(\mathbf{b}, \mathbf{A})$  and  $(\mathbf{b}, \mathbf{A}')$ , by similar induction procedure as buyers, we have

$$\Pr[M(\mathbf{b}, \mathbf{A}) = \mathbf{p}] / \Pr[M(\mathbf{b}, \mathbf{A}') = \mathbf{p}] \leq \exp(\varepsilon).$$

Thus, the DPAM is  $\varepsilon$ -differentially private to sellers, and Theorem 1 has been proven.  $\square$

To achieve the  $\gamma$ -truthfulness eventually, we first introduce the following two lemmas as a foreshadowing.

**Lemma 1.** *Given a clearing price  $\mathbf{p} \in \Theta^k$ , for each buyer  $TD_i \in \mathbb{T}\mathbb{D}$ , the DPAM achieves*

$$u_i^{TD}((v_i, \Omega_{-i}), \mathbf{p}) \geq u_i^{TD}((b_i, \Omega_{-i}), \mathbf{p}). \quad (16)$$

*Proof.* The  $TD_i \in \mathbb{T}\mathbb{D}_c$  if it bids truthfully. There are two sub-cases we need to concern:

- $b_i > v_i$ : The  $TD_i$  will be in  $\mathbb{T}\mathbb{D}_c$  as well. According to the winner candidate determination and assignment, the auction result to the  $TD_i$  will not change. Thus, we have  $u_i^{TD}((v_i, \Omega_{-i}), \mathbf{p}) = u_i^{TD}((b_i, \Omega_{-i}), \mathbf{p})$ .
- $b_i < v_i$ : If  $\sum_{z=1}^k p_z \cdot d_i^z \leq b_i$  can be satisfied, the  $TD_i$  will be in  $\mathbb{T}\mathbb{D}_c$  as well. Thus, we

have  $u_i^{TD}((v_i, \Omega_{-i}), \mathbf{p}) = u_i^{TD}((b_i, \Omega_{-i}), \mathbf{p})$ ; Otherwise, the  $TD_i$  will be not in  $\mathbb{T}\mathbb{D}_c$ , which loses the auction definitely. Thus, we have  $u_i^{TD}((v_i, \Omega_{-i}), \mathbf{p}) \geq u_i^{TD}((b_i, \Omega_{-i}), \mathbf{p}) = 0$ .

The  $TD_i \notin \mathbb{T}\mathbb{D}_c$  if it bids truthfully. There are two sub-cases we need to concern:

- $b_i > v_i$ : If  $\sum_{z=1}^k p_z \cdot d_i^z \leq b_i$  can be satisfied, the  $TD_i$  will be in  $\mathbb{T}\mathbb{D}_c$ . If it can be assigned an edge node in the assignment stage, its utility will be  $u_i^{TD}((b_i, \Omega_{-i}), \mathbf{p}) = v_i - \sum_{z=1}^k p_z \cdot d_i^z < 0 = u_i^{TD}((v_i, \Omega_{-i}), \mathbf{p})$ .
- $b_i < v_i$ : The  $TD_i$  will be not in  $\mathbb{T}\mathbb{D}_c$  as well, which loses the auction definitely. Thus, we have  $u_i^{TD}((v_i, \Omega_{-i}), \mathbf{p}) = u_i^{TD}((b_i, \Omega_{-i}), \mathbf{p}) = 0$ .

From the above, we always have  $u_i^{TD}((v_i, \Omega_{-i}), \mathbf{p}) \geq u_i^{TD}((b_i, \Omega_{-i}), \mathbf{p})$ , and Lemma 1 has been proven.  $\square$

**Lemma 2.** *Given a clearing price  $\mathbf{p} \in \Theta^k$ , for each buyer  $EN_j \in \mathbb{E}\mathbb{N}$ , the DPAM achieves*

$$u_j^{EN}((c_j, \Omega_{-j}), \mathbf{p}) \geq u_j^{EN}((a_j, \Omega_{-j}), \mathbf{p}). \quad (17)$$

*Proof.* First, “ $a_j > c_j$ ” implies there is at least one element in these vectors satisfying  $a_j^{z^*} > c_j^{z^*}$  and others satisfy  $a_j^z \geq c_j^z$  for each  $r_z \in \mathbb{R} \setminus \{r_{z^*}\}$ . Second, we denoted by  $x_{ij} \in \bar{\mathbf{X}}$  the allocation when a seller asks truthfully and  $\bar{x}_{ij} \in \bar{\mathbf{X}}$  the allocation when a seller asks untruthfully.

Consider the seller  $EN_j \in \mathbb{E}\mathbb{N}$ , there are two sub-cases we need to concern:

- $a_j > c_j$ : When  $x_{ij} = 1$ , the auction result will be  $\bar{x}_{ij} = 1$  as well if  $\sum_{z=1}^k (p_z - a_z) \cdot d_i^z \geq 0$  can be satisfied; otherwise  $\bar{x}_{ij} = 0$ . Thus, we have  $u_j^{EN}((c_j, \Omega_{-j}), \mathbf{p}) \geq u_j^{EN}((a_j, \Omega_{-j}), \mathbf{p})$  because  $x_{ij} \geq \bar{x}_{ij}$ .
- $a_j < c_j$ : When  $x_{ij} = 1$ , the auction result will be  $\bar{x}_{ij} = 1$  as well. When  $x_{ij} = 0$  and  $\sum_{z=1}^k (p_z - c_z) \cdot d_i^z \geq 0$ , the auction result to the  $\bar{x}_{ij} = 0$  will not change according to the assignment. However, when  $x_{ij} = 0$  and  $\sum_{z=1}^k (p_z - c_z) \cdot d_i^z < 0$ , it is possible to happen  $\sum_{z=1}^k (p_z - c_z) \cdot d_i^z \geq 0$ , and leading to  $\bar{x}_{ij} = 1$  if  $\delta_{ij}$  is the minimum one among this buyer's winning seller candidates. The utility gained from  $TD_i$  less than zero. Thus, we have  $u_j^{EN}((c_j, \Omega_{-j}), \mathbf{p}) \geq u_j^{EN}((a_j, \Omega_{-j}), \mathbf{p})$ .

From the above, we always have  $u_j^{EN}((c_j, \Omega_{-j}), \mathbf{p}) \geq u_j^{EN}((a_j, \Omega_{-j}), \mathbf{p})$ , and Lemma 2 has been proven.  $\square$

**Theorem 2.** *The DPAM achieves  $\gamma$ -truthfulness.*

*Proof.* Given two neighboring inputs  $(\mathbf{b}, \mathbf{A})$  and  $(\mathbf{b}', \mathbf{A})$ , for any buyer  $TD_i \in \mathbb{T}\mathbb{D}$ , we assume that  $v_i \in \mathbf{b}$  and  $b_i \in \mathbf{b}'$ . Thus, we have

$$\begin{aligned} & \mathbb{E}[u_i^{TD}(v_i, \Omega_{-i})] \\ &= \sum_{\mathbf{p} \in \Theta^k} \Pr[M(\mathbf{b}, \mathbf{A}) = \mathbf{p}] \cdot u_i^{TD}((v_i, \Omega_{-i}), \mathbf{p}) \\ &\geq \exp(-\varepsilon) \cdot \sum_{\mathbf{p} \in \Theta^k} \Pr[M(\mathbf{b}', \mathbf{A}) = \mathbf{p}] \cdot u_i^{TD}((b_i, \Omega_{-i}), \mathbf{p}) \\ &= \exp(-\varepsilon) \cdot \mathbb{E}[u_i^{TD}(b_i, \Omega_{-i})] \\ &\geq (1 - \varepsilon) \cdot \mathbb{E}[u_i^{TD}(b_i, \Omega_{-i})] \\ &\geq \mathbb{E}[u_i^{TD}(b_i, \Omega_{-i})] - \varepsilon \cdot v_{max}. \end{aligned}$$

For any buyer  $TD_i \in \mathbb{TD}$ , we have  $\mathbb{E}[u_i^{TD}(b_i, \Omega_{-i})] \leq \max_{TD_i \in \mathbb{TD}} \{u_i^{TD}\} \leq v_{max} - c_{min} \cdot \min_{TD_i \in \mathbb{TD}} \{\sum_{z=1}^k d_i^z\} \leq v_{max}$ . Thus, we can conclude that the DPAM achieves  $\varepsilon \cdot v_{max}$ -truthfulness to buyers.

Given two neighboring inputs  $(\mathbf{b}, \mathbf{A})$  and  $(\mathbf{b}, \mathbf{A}')$ , for any seller  $EN_j \in \mathbb{EN}$ , we assume that  $\mathbf{c}_j \in \mathbf{A}$  and  $\mathbf{a}_j \in \mathbf{A}'$ . Similarly as the above, we have

$$\begin{aligned} & \mathbb{E}[u_j^{EN}(\mathbf{c}_j, \Omega_{-j})] \\ & \geq \mathbb{E}[u_j^{EN}(\mathbf{a}_j, \Omega_{-j})] - \varepsilon \cdot (c_{max} - c_{min}) \cdot k \cdot h_{max}. \end{aligned}$$

For any seller  $EN_j \in \mathbb{EN}$ , we have  $\mathbb{E}[u_j^{EN}(\mathbf{c}_j, \Omega_{-j})] \leq \max_{EN_j \in \mathbb{EN}} \{u_j^{EN}\} \leq (c_{max} - c_{min}) \cdot \sum_{z=1}^k h_j^z \leq (c_{max} - c_{min}) \cdot k \cdot h_{max}$ . Thus, we can conclude that the DPAM achieves  $\varepsilon \cdot (c_{max} - c_{min}) \cdot k \cdot h_{max}$ -truthfulness to sellers.

Giving  $\gamma = \max\{\varepsilon \cdot v_{max}, \varepsilon \cdot (c_{max} - c_{min}) \cdot k \cdot h_{max}\}$ , the DPAM achieve  $\gamma$ -truthfulness.  $\square$

**Theorem 3.** *The DPAM achieves individual rationality.*

*Proof.* According to Theorem 2, no player has the motivation to bid/ask untruthfully. We can consider  $b_i = v_i$  for each buyer  $TD_i \in \mathbb{TD}$  and  $\mathbf{a}_j = \mathbf{c}_j$  for each seller  $EN_j \in \mathbb{EN}$ . Based on the winning candidate determination, each winning buyer  $TD_i$  must have  $\sum_{z=1}^k p_z \cdot d_i^z \leq b_i$ , thus its utility  $u_i^{TD} \geq 0$ . Based on the assignment, each winning seller  $EN_j$  that provides resources to buyer  $TD_i$  must have  $\sum_{z=1}^k (p_z - a_z) \cdot d_i^z \geq 0$ , which means that providing resources to an IoT devices always bring positive returns. Thus, its utility  $u_j^{EN} \geq 0$ .  $\square$

**Theorem 4.** *The DPAM achieves budget balanced.*

*Proof.* The utilities of all edge nodes are positive according to Theorem 3, thus the sum of them (budget)  $\sum_{j=1}^n u_j^{EN}$  is greater than zero as well.  $\square$

**Theorem 5.** *The DPAM does not achieve computational efficiency.*

*Proof.* The main loop to traverse all possible price vectors  $\mathbf{p} \in \Theta^k$  contains  $|\Theta^k|$  iterations. For each iteration, the dominant step in winning candidate determination is to sort  $\mathbb{TD}_c$ , which has at most  $m$  elements. Thus, sorting  $\mathbb{TD}_c$  is bounded by  $O(m \log m)$ . Then, in the assignment, it takes  $O(n)$  for each buyer  $TD_i \in \mathbb{TD}_c$ . Thus, its running time is bounded by  $O(mn)$ . The total time complexity of Algorithm 1 is bounded by  $O((mn + m \log m) \cdot |\Theta^k|)$ . Therefore, the running time increases exponentially with  $k$  instead of polynomial time.  $\square$

Next, we need to calculate the expected performance of our proposed mechanism. Based on (13), the expected revenue of edge computing platform can be expressed as

$$\mathbb{E}[R(\mathbf{b}, \mathbf{A})] = \sum_{\mathbf{p} \in \Theta^k} \Pr[M(\mathbf{b}, \mathbf{A}) = \mathbf{p}] \cdot R((\mathbf{b}, \mathbf{A}), \mathbf{p}). \quad (18)$$

To achieve the approximation ratio of the DPAM, we first introduce the following lemma.

**Lemma 3.** *Let  $OPT$  be the optimal revenue by solving the problem defined in (4) and  $OPT^* = \max_{\mathbf{p} \in \Theta^k} \{R((\mathbf{b}, \mathbf{A}), \mathbf{p})\}$  be the maximum revenue obtained by the winning candidate*

*determination and assignment process of Algorithm 1. Then, we have*

$$F(\Theta) \cdot OPT \leq OPT^* \leq OPT \quad (19)$$

*where we denoted by  $F(\Theta) = \frac{\max_{\mathbf{p} \in \Theta^k} \{R((\mathbf{b}, \mathbf{A}), \mathbf{p})\}}{(c_{max} - c_{min}) \cdot n \cdot k \cdot h_{max}}$  as a factor of  $OPT$ .*

*Proof.* Because the  $OPT$  is globally optimal, we must have  $OPT \geq OPT^*$ . Based on (4), we have

$$OPT \leq (c_{max} - c_{min}) \cdot n \cdot k \cdot h_{max} \quad (20)$$

since each edge node provides at most  $k \cdot h_{max}$  units of resources and there are total  $n$  edge nodes. According to the definition of  $OPT^*$ , we have

$$\begin{aligned} OPT^* &= \max_{\mathbf{p} \in \Theta^k} \{R((\mathbf{b}, \mathbf{A}), \mathbf{p})\} \\ &\geq \frac{\max_{\mathbf{p} \in \Theta^k} \{R((\mathbf{b}, \mathbf{A}), \mathbf{p})\}}{(c_{max} - c_{min}) \cdot n \cdot k \cdot h_{max}} \cdot OPT \\ &= F(\Theta) \cdot OPT \end{aligned}$$

since the relationship (20) exists.  $\square$

In order to achieve the truthfulness, the returned revenue is not optimal even though there is no differential privacy. This difference can be bounded by  $F(\Theta)$ . After introducing the differential privacy, the revenue will be damaged further.

**Theorem 6.** *The expected revenue of edge computing platform  $\mathbb{E}[R(\mathbf{b}, \mathbf{A})]$  achieved by DPAM and the optimal revenue  $OPT$  satisfies that  $\mathbb{E}[R(\mathbf{b}, \mathbf{A})] \geq$*

$$F(\Theta) \cdot OPT - \frac{6\Delta R}{\varepsilon} \cdot \ln \left( e + \frac{\varepsilon OPT |\Theta^k|}{2\Delta R} \right). \quad (21)$$

*Proof.* Let  $OPT^* = \max_{\mathbf{p} \in \Theta^k} \{R((\mathbf{b}, \mathbf{A}), \mathbf{p})\}$  be the maximum revenue returned by the DPAM. For a small constant  $t \geq 0$ , we define four sets, which are  $S_t = \{\mathbf{p} : R((\mathbf{b}, \mathbf{A}), \mathbf{p}) > OPT^* - t\}$ ,  $\bar{S}_t = \{\mathbf{p} : R((\mathbf{b}, \mathbf{A}), \mathbf{p}) \leq OPT^* - t\}$ ,  $S_{2t} = \{\mathbf{p} : R((\mathbf{b}, \mathbf{A}), \mathbf{p}) > OPT^* - 2t\}$ , and  $\bar{S}_{2t} = \{\mathbf{p} : R((\mathbf{b}, \mathbf{A}), \mathbf{p}) \leq OPT^* - 2t\}$ . Thus, we have  $\Pr[M(\mathbf{b}, \mathbf{A}) \in \bar{S}_{2t}] \leq$

$$\begin{aligned} & \leq \frac{\Pr[M(\mathbf{b}, \mathbf{A}) \in \bar{S}_{2t}]}{\Pr[M(\mathbf{b}, \mathbf{A}) \in S_t]} \\ &= \frac{\sum_{\mathbf{p} \in \bar{S}_{2t}} \frac{\exp\left(\frac{\varepsilon R((\mathbf{b}, \mathbf{A}), \mathbf{p})}{2\Delta R}\right)}{\sum_{\mathbf{p}' \in \Theta^k} \exp\left(\frac{\varepsilon R((\mathbf{b}, \mathbf{A}), \mathbf{p}')}{2\Delta R}\right)}}{\sum_{\mathbf{p} \in S_t} \frac{\exp\left(\frac{\varepsilon R((\mathbf{b}, \mathbf{A}), \mathbf{p})}{2\Delta R}\right)}{\sum_{\mathbf{p}' \in \Theta^k} \exp\left(\frac{\varepsilon R((\mathbf{b}, \mathbf{A}), \mathbf{p}')}{2\Delta R}\right)}} \\ &= \frac{\sum_{\mathbf{p} \in \bar{S}_{2t}} \exp\left(\frac{\varepsilon R((\mathbf{b}, \mathbf{A}), \mathbf{p})}{2\Delta R}\right)}{\sum_{\mathbf{p} \in S_t} \exp\left(\frac{\varepsilon R((\mathbf{b}, \mathbf{A}), \mathbf{p})}{2\Delta R}\right)} \leq \frac{|\bar{S}_{2t}| \cdot \exp\left(\frac{\varepsilon(OPT^* - 2t)}{2\Delta R}\right)}{|S_t| \cdot \exp\left(\frac{\varepsilon(OPT^* - t)}{2\Delta R}\right)} \\ &= \frac{|\bar{S}_{2t}|}{|S_t|} \cdot \exp\left(\frac{-\varepsilon t}{2\Delta R}\right). \end{aligned} \quad (22)$$

Based on (22), we have

$$\begin{aligned} \Pr[M(\mathbf{b}, \mathbf{A}) \in S_{2t}] &\geq 1 - \frac{|\bar{S}_{2t}|}{|S_t|} \cdot \exp\left(\frac{-\varepsilon t}{2\Delta R}\right) \\ &\geq 1 - |\Theta^k| \cdot \exp\left(\frac{-\varepsilon t}{2\Delta R}\right) \end{aligned} \quad (23)$$



since  $\Pr[M(\mathbf{b}, \mathbf{A}) \in S_{2t}] + \Pr[M(\mathbf{b}, \mathbf{A}) \in \bar{S}_{2t}] = 1$ ,  $|\bar{S}_{2t}| \leq |\Theta^k|$ , and  $|S_t| \geq 1$ . Thus, the expected revenue  $\mathbb{E}[R(\mathbf{b}, \mathbf{A})]$  can be expressed as

$$\begin{aligned} \mathbb{E}[R(\mathbf{b}, \mathbf{A})] &\geq \sum_{\mathbf{p} \in S_{2t}} \Pr[M(\mathbf{b}, \mathbf{A}) = \mathbf{p}] \cdot R((\mathbf{b}, \mathbf{A}), \mathbf{p}) \\ &\geq \Pr[M(\mathbf{b}, \mathbf{A}) \in S_{2t}] \cdot (OPT^* - 2t) \\ &\geq \left[1 - |\Theta^k| \cdot \exp\left(\frac{-\varepsilon t}{2\Delta R}\right)\right] \cdot (OPT^* - 2t) \end{aligned}$$

For any  $t$  satisfying

$$t \geq \frac{2\Delta R}{\varepsilon} \cdot \ln\left(\frac{|\Theta^k| OPT^*}{t}\right) \quad (24)$$

we have  $\exp\left(\frac{-\varepsilon t}{2\Delta R}\right) \leq \frac{t}{OPT^* |\Theta^k|}$ . Thus,

$$\begin{aligned} \mathbb{E}[R(\mathbf{b}, \mathbf{A})] &\geq \left(1 - |\Theta^k| \cdot \frac{t}{OPT^* |\Theta^k|}\right) \cdot (OPT^* - 2t) \\ &= OPT^* - 3t + \frac{2t^2}{OPT^*} \\ &\geq OPT^* - 3t. \end{aligned} \quad (25)$$

By giving  $t = \frac{2\Delta R}{\varepsilon} \ln\left(e + \frac{\varepsilon OPT^* |\Theta^k|}{2\Delta R}\right)$ , we have

$$\begin{aligned} t &= \frac{2\Delta R}{\varepsilon} \cdot \ln\left(e + \frac{\varepsilon OPT^* |\Theta^k|}{2\Delta R}\right) \\ &\geq \frac{2\Delta R}{\varepsilon} \cdot \ln\left(OPT^* |\Theta^k| \frac{\varepsilon}{2\Delta R}\right) \\ &\geq \frac{2\Delta R}{\varepsilon} \cdot \ln\left(\frac{|\Theta^k| OPT^*}{t}\right) \end{aligned}$$

where it satisfies (24) because  $\ln\left(e + \frac{\varepsilon OPT^* |\Theta^k|}{2\Delta R}\right) \geq 1$  and  $t \geq \frac{2\Delta R}{\varepsilon}$ . Finally, we substitute  $t = \frac{2\Delta R}{\varepsilon} \cdot \ln\left(e + \frac{\varepsilon OPT^* |\Theta^k|}{2\Delta R}\right)$  into (25), we have

$$\begin{aligned} \mathbb{E}[R(\mathbf{b}, \mathbf{A})] &\geq OPT^* - 3t \\ &\geq OPT^* - \frac{6\Delta R}{\varepsilon} \cdot \ln\left(e + \frac{\varepsilon OPT^* |\Theta^k|}{2\Delta R}\right) \\ &\geq F(\Theta) \cdot OPT - \frac{6\Delta R}{\varepsilon} \cdot \ln\left(e + \frac{\varepsilon OPT |\Theta^k|}{2\Delta R}\right). \end{aligned}$$

Therefore, Theorem 6 has been proven.  $\square$

## VI. IMPLEMENTATION AND SIMULATION

Shown as Theorem 5, the running time of Algorithm 1 can be bounded by  $|\Theta^k|$ , which is not computationally efficient. Thus, in this section, we first discuss an implementation technique to reduce the time complexity to polynomial time. Then, we implement and evaluate our proposed mechanism by extensive simulations.

### A. Implementation Technique

In order to reduce the running time, we can learn from the recent research in [13] to select the unit price of each resource one by one instead of selecting the price vector. The procedure is shown in Algorithm 2.

First of all, we define an average unit bid of each buyer  $TD_i \in \mathbb{TD}$  as  $\bar{b}_i = b_i / (\sum_{z=1}^k d_i^z)$ . The main loop that iterates

### Algorithm 2 DPAM-S

---

**Input:**  $(\{\mathcal{B}_i\}_{TD_i \in \mathbb{TD}}, \{\mathcal{A}_j\}_{EN_j \in \mathbb{EN}})$ ,  $\varepsilon$ ,  $\Theta$

**Output:**  $\mathbf{X}_{\mathbf{p}}, \mathbf{p}$

- 1: Initialize  $\bar{b}_i = b_i / (\sum_{z=1}^k d_i^z)$  for each  $TD_i \in \mathbb{TD}$
- 2: Initialize  $\varepsilon' = \varepsilon / k$
- 3: **for**  $\ell \leftarrow 1$  to  $k$  **do**
- 4:   Initialize  $\Delta R^\ell = \sum_{j=1}^n (c_{max} - c_{min}) \cdot \sum_{z=1}^\ell h_j^z$
- 5:   **for** each  $p_\ell \in \Theta$  **do**
- 6:     Initialize  $x_{ij} = 0$  for each  $x_{ij} \in \mathbf{X}_{\ell, p_\ell}$
- 7:     Initialize  $\mathbb{TD}_c^\ell \leftarrow \emptyset$
- 8:     **for** each  $TD_i \in \mathbb{TD}$  **do**
- 9:       **if**  $\sum_{z=1}^\ell p_z \cdot d_i^z \leq \bar{b}_i \cdot \sum_{z=1}^\ell d_i^z$  **then**
- 10:          $\mathbb{TD}_c^\ell \leftarrow \mathbb{TD}_c^\ell \cup \{TD_i\}$
- 11:       **end if**
- 12:     **end for**
- 13:     Sort the  $\mathbb{TD}_c^\ell$  s.t.  $\sum_{z=1}^k d_1^z \geq \sum_{z=1}^k d_2^z \geq \dots$
- 14:     Initialize  $\{h_j^{1'}, h_j^{2'}, \dots, h_j^{\ell'}\}$  where  $h_j^{z'} = h_j^z \in \mathbb{H}_j$
- 15:     **for** each  $TD_i \in \mathbb{TD}_c^\ell$  **do**
- 16:       Initialize  $\mathbb{EN}_{c,i}^\ell \leftarrow \emptyset$
- 17:       **for** each  $EN_j \in \mathbb{EN}$  **do**
- 18:         **if**  $h_j^{z'} \geq d_i^z$  for each  $r_z \in \{r_1, \dots, r_\ell\}$ ,  $\delta_{ij} \leq dm_i$ , and  $\sum_{z=1}^\ell (p_z - a_z) \cdot d_i^z \geq 0$  **then**
- 19:            $\mathbb{EN}_{c,i}^\ell \leftarrow \mathbb{EN}_{c,i}^\ell \cup \{EN_j\}$
- 20:         **end if**
- 21:       **end for**
- 22:       **if**  $\mathbb{EN}_{c,i}^\ell \neq \emptyset$  **then**
- 23:          $EN_{j^*} \leftarrow \arg \min_{EN_j \in \mathbb{EN}_{c,i}^\ell} \{\delta_{ij}\}$
- 24:         **for** each  $r_z \in \{r_1, \dots, r_\ell\}$  **do**
- 25:            $h_{j^*}^{z'} \leftarrow h_{j^*}^{z'} - d_i^z$
- 26:         **end for**
- 27:          $x_{ij^*} \leftarrow 1$
- 28:       **end if**
- 29:     **end for**
- 30:      $R^\ell((\mathbf{b}, \mathbf{A}), p_\ell) = \sum_{j=1}^n [\sum_{z=1}^\ell (p_z - a_j^z) \sum_{i=1}^m x_{ij} d_i^z]$
- 31:   **end for**
- 32:   Select a  $p_\ell \in \Theta$  according to the selection distribution:
 
$$\Pr[M^\ell(\mathbf{b}, \mathbf{A}) = p_\ell] = \frac{\exp\left(\frac{\varepsilon' R^\ell((\mathbf{b}, \mathbf{A}), p_\ell)}{2\Delta R^\ell}\right)}{\sum_{p'_\ell \in \Theta} \exp\left(\frac{\varepsilon' R^\ell((\mathbf{b}, \mathbf{A}), p'_\ell)}{2\Delta R^\ell}\right)}$$
- 33: **end for**
- 34: **return**  $\mathbf{X}_{k, p_k}, \mathbf{p} = \{p_1, p_2, \dots, p_k\}$

---

$k$  times to check all kinds of resources. When checking the  $\ell$ -th unit price  $p_\ell \in \Theta$  ( $1 \leq \ell \leq k$ ), we have known the previous first  $\ell - 1$  unit pricings. A partial price vector  $(p_1, p_2, \dots, p_{\ell-1})$  has been determined. Given a unit price  $p_\ell \in \Theta$ , we select partial winning buyer candidates  $\mathbb{TD}_c^\ell \subseteq \mathbb{TD}$  such that for each buyer  $TD_i \in \mathbb{TD}_c^\ell$ , we have

$$\sum_{z=1}^\ell p_z \cdot d_i^z \leq \bar{b}_i \cdot \sum_{z=1}^\ell d_i^z. \quad (26)$$

Then, it generates an allocation matrix  $\mathbf{X}_{\ell, p_\ell}$  similar to the DPAM. The partial revenue can be calculate by

$$R^\ell((\mathbf{b}, \mathbf{A}), p_\ell) = \sum_{j=1}^n \left[ \sum_{z=1}^\ell (p_z - a_j^z) \cdot \sum_{i=1}^m x_{ij} \cdot d_i^z \right]. \quad (27)$$

Here, the sensitivity of partial score function  $R^\ell(\cdot)$  can be written as  $\Delta R^\ell = \sum_{j=1}^n (c_{max} - c_{min}) \cdot \sum_{z=1}^{\ell} h_j^z$ . According to the exponential mechanism, the probability distribution of selection a unit price  $p_\ell \in \Theta$  can be defined as follows.

$$\Pr[M^\ell(\mathbf{b}, \mathbf{A}) = p_\ell] = \frac{\exp\left(\frac{\varepsilon' R^\ell((\mathbf{b}, \mathbf{A}), p_\ell)}{2\Delta R^\ell}\right)}{\sum_{p'_\ell \in \Theta} \exp\left(\frac{\varepsilon' R^\ell((\mathbf{b}, \mathbf{A}), p'_\ell)}{2\Delta R^\ell}\right)} \quad (28)$$

where  $\varepsilon' = \varepsilon/k$ . Therefore, the time complexity is reduced from  $O((mn + m \log m) \cdot |\Theta^k|)$  to  $O((mn + m \log m) \cdot k|\Theta|)$  according to Algorithm 2.

**Theorem 7.** *The DPAM-S achieves  $\varepsilon$ -differential privacy,  $\gamma$ -truthfulness, individual rationality, budget balanced, computational efficiency. Moreover, the expected revenue  $\mathbb{E}[R^k(\mathbf{b}, \mathbf{A})]$  achieved by DPAM-S satisfies that  $\mathbb{E}[R^k(\mathbf{b}, \mathbf{A})] \geq$*

$$F(\Theta) \cdot OPT - \frac{6k\Delta R}{\varepsilon} \cdot \ln\left(e + \frac{\varepsilon OPT|\Theta|}{2\Delta R}\right). \quad (29)$$

*Proof.* Based on Theorem 1 to Theorem 6 in this paper and Theorem 7 in [13], this theorem can be proven.  $\square$

There are two mechanisms, DPAM and DPAM-S, to maximize the revenue of edge computing platform and satisfy desirable properties. Given a fixed privacy budget  $\varepsilon$ , the revenue achieved by DPAM is better, but the running time of DPAM-S is better. Which mechanism is better depends on the requirements between performance and running time.

### B. Simulation Setup

To simulate this scenario, we construct a virtual rectangular region with  $1000 \times 1000$ , where there are  $m$  IoT devices and  $n$  edge nodes distributed in this area uniformly. For each  $TD_i \in \mathbb{T}\mathbb{D}$ , we define its coordinate as  $(x_i, y_i)$ . Similarly, we have  $(x_j, y_j)$  for each  $EN_j \in \mathbb{E}\mathbb{N}$ . The distance  $\delta_{ij}$  between IoT device  $TD_i$  and edge node  $EN_j$  can be written as  $\delta_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$ . For each buyer  $TD_i \in \mathbb{T}\mathbb{D}$ , its bidding information contains a maximum permitted distance  $dm_i$ , which is distributed in  $[200\sqrt{2}, 1000\sqrt{2}]$  uniformly since the maximum distance between IoT devices and edge nodes is  $1000\sqrt{2}$  in this area.

Suppose the price of a unit of resources can be normalized in  $[0, 1]$ , then  $\Theta = [c_{min}, c_{max}] = [0, 1]$ . To implement our mechanisms, the first step is to discretize this interval  $[0, 1]$  so as to traverse all possible price vectors in the space  $\Theta^k$ . Here, we define a concept called “granularity”, denoted by  $\sigma$ . The  $\sigma = 0.02$  implies that we divide the interval  $[0, 1]$  equally into fifty parts, that is  $\Theta = \{0, 0.02, 0.04, \dots, 0.98, 1\}$ . The granularity can be used as an effective method to balance the performance and time complexity. Since  $\Theta = [0, 1]$ , we sample  $a_j^z$  for each seller  $EN_j \in \mathbb{E}\mathbb{N}$  and  $r_z \in \mathbb{R}$  uniformly in  $[0, 1]$ . Next, we assume the number of resource types  $k \in \{1, 2, \dots, 5\}$ , and the available range of each resource  $[h_{min}, h_{max}] = [0, 20]$ . Therefore, in the simulation, we make  $h_j^z \in \mathbb{H}_j$  for each seller  $EN_j \in \mathbb{E}\mathbb{N}$  and  $r_z \in \mathbb{R}$  distributed in  $[10, 20]$  uniformly. Similarly, we assume the  $[d_{min}, d_{max}] = [1, 5]$ , thus we make  $d_i^z \in \mathbb{D}_i$  for each buyer  $TD_i \in \mathbb{T}\mathbb{D}$  and  $r_z \in \mathbb{R}$  distributed in  $[1, 5]$  uniformly.

In the next step, we need to discuss how buyers decide their total bids. That is, how can we sample a total bid  $b_i$  for each buyer  $TD_i \in \mathbb{T}\mathbb{D}$ . According to our preceding description, the average price per unit resource is  $(1 + 0)/2 = 0.5$ . Here, we point out a reasonable assumption that the total bid is related to the total demand of the buyer for resources. Thus, we can sample the  $b_i$  for each buyer  $TD_i \in \mathbb{T}\mathbb{D}$  as follows:

$$b_i = (0.5) \cdot \sum_{z=1}^k d_i^z \cdot U(0.7, 1.3) \quad (30)$$

where the  $U(0.7, 1.3)$  is a value sampled from the interval  $[0.7, 1.3]$  uniformly.

Due to the introduction of differential privacy, the auction results have certain randomness. Thus, given a mechanism, its result is the average value of 500 trials. To analyze the performance of our mechanisms based on differential privacy, we need a reference. For example in line 32 of Algorithm 1, we select a  $\mathbf{p} \in \Theta^k$  such that maximizing  $R((\mathbf{b}, \mathbf{A}), \mathbf{p})$  as the final result. By removing the randomness (differential privacy) of the DPAM and DPAM-S, we can define two deterministic auction mechanisms, marked by “DTAM” and “DTAM-S”, as references. Here, “DT” implies “deterministic”. Finally, we select three typical metrics to evaluate the performance of our proposed mechanisms, which are shown as follows.

- 1) Expected revenue of edge computing platform: it can be computed by (18).
- 2) Expected satisfaction: the ratio of the number of satisfied IoT devices to the total number of IoT devices.
- 3) Running time: the time taken to execute a trial.

### C. Simulation Results and Analysis

In any time slot  $t \in T$ , there are  $m$  IoT devices (buyers) and  $n$  edge nodes. Generally, the number of IoT devices is much larger than that of edge nodes, thus we assume that  $m \geq n$  in our following simulations. Our task in this part can be divided into four parts, which discuss the impact of granularity, the number of resource types, the number of IoT devices, and privacy budget on the performance of our proposed mechanisms respectively.

**Granularity:** Figure 2 plots the revenues, satisfactions, and running times of four different mechanisms vary with the increase of granularity, where we assume  $m = 100$ ,  $n = 10$ ,  $k = 3$ , and  $\varepsilon = 200$ . Shown as Figure 2 (a), we can see that the revenue will decrease slightly with the increase of granularity. This is because smaller granularity means higher accuracy, thus we can compute more price vectors and select the better one. Similar results are also reflected in users’ satisfaction. Shown as Figure 2 (c), the running time will increase significantly with the decrease of granularity. Here, let us make a rough analysis. Supposing  $\sigma_1 = 0.1 \cdot \sigma_2$ , we have  $|\Theta_1| = 10 \cdot |\Theta_2|$ . In the DPAM (DTAM), the running time under the granularity  $\sigma_1$  is  $10^k$  times as much as that under the granularity  $\sigma_2$ . And in the DPAM-S (DPTM-S), the running time under the granularity  $\sigma_1$  is  $10 \cdot k$  times as much as that under the granularity  $\sigma_2$ . The simulation results in Figure 3 (c) meets our expectations in general. We have mentioned that the granularity is a method to balance performance and

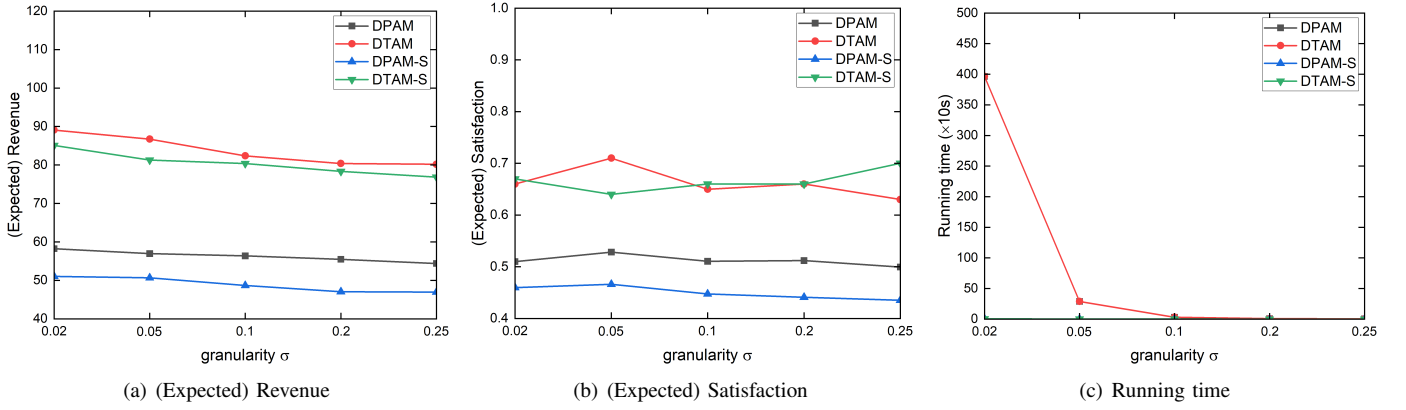


Fig. 2. The performances of proposed mechanisms on different granularities, where  $m = 100$ ,  $n = 50$ ,  $k = 3$ , and  $\varepsilon = 200$ .

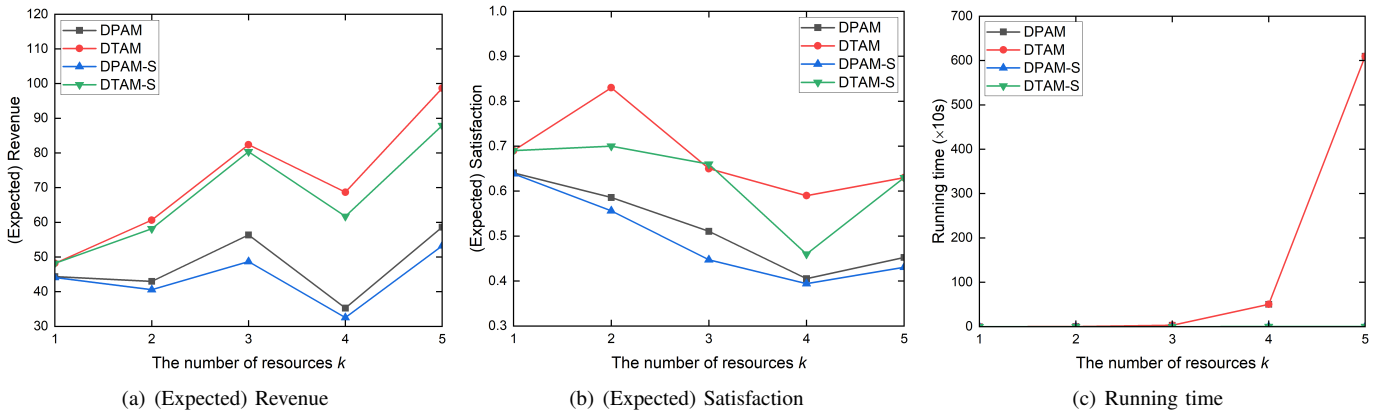


Fig. 3. The performances of proposed mechanisms on different number of resource types, where  $m = 100$ ,  $n = 50$ ,  $\sigma = 0.1$ , and  $\varepsilon = 200$ .

time complexity. Based on the results of Figure 2, we set the granularity  $\sigma = 0.1$  in the following simulations.

**The number of resource types:** Figure 3 plots the performances vary with the increasing number of resource types, where we assume  $m = 100$ ,  $n = 10$ ,  $\sigma = 0.1$ , and  $\varepsilon = 200$ . Shown as Figure 3 (a), we observe that the revenue will show an upward trend with the increase of resource types. This is because the increase in resource types enables each edge nodes to sell more resource units. However, there is an exception when  $k = 4$ . From Figure 3 (b), we can see that the users' satisfaction drops obviously when  $k = 4$ . This may be due to the randomness of data, which makes the resource request of IoT devices difficult to realize, which leads to the decline of their satisfaction. In addition, another important discovery is that the gap between DPAM (DPAM-S) and DTAM (DTAM-S) increases with the increase of resource types. Under a larger  $k$ , the sample space  $\Theta^k$  will become larger, resulting in higher randomness. In other words, the probability of choosing the optimal solution will become smaller. Shown as Figure 3 (c), the running time will increase significantly with the increasing number of resource types. Similarly, we suppose  $k_1 = k_2 + 1$ . In the DPAM (DTAM), the running time under the  $k_1$  is  $|\Theta|$  times as much as that under the  $k_2$  since we have  $|\Theta|^{k_1} = |\Theta|^{k_2} \cdot |\Theta|$ . And in the DPAM-S (DTAM-S), the running time under the  $k_1$  is  $(k_2 + 1)/k_2$  times as much

as that under the  $k_2$ . If there are a large number of resource types, the DPAM (DTAM) is undesirable since its running time grows exponentially. By contrast, the running time of DPAM-S (DTAM-S) grows linearly.

**The number of IoT devices:** Figure 4 plots the revenues, satisfactions, and running times of four different mechanisms vary with the increasing number of IoT devices, where we assume  $n = 10$ ,  $k = 3$ ,  $\sigma = 0.1$ , and  $\varepsilon = 200$ . Shown as Figure 4 (a) and (b), we can see that the revenue will increase and the satisfaction will decrease with the increasing number of IoT devices. This is because there are more feasible buyer candidates requesting resources, so that the resources of edge nodes can be more fully utilized. Although more IoT devices can be satisfied, the total number of IoT devices becomes much more, resulting in a decline in satisfaction. Shown as Figure 4 (c), the running time will grow linearly with the increasing number of IoT devices, which meets our expectations in general.

**Privacy budget:** Figure 5 plots the performances vary with the increase of privacy budget, where we assume  $m = 100$ ,  $n = 10$ ,  $k = 3$ , and  $\sigma = 0.1$ . Shown as Figure 5 (a) and (b), we observe that the revenue and satisfaction remain unchanged in the DTAM and DTAM-S since they are deterministic mechanisms and have nothing to do with the value of privacy budget. In the DPAM and DPAM-S, the

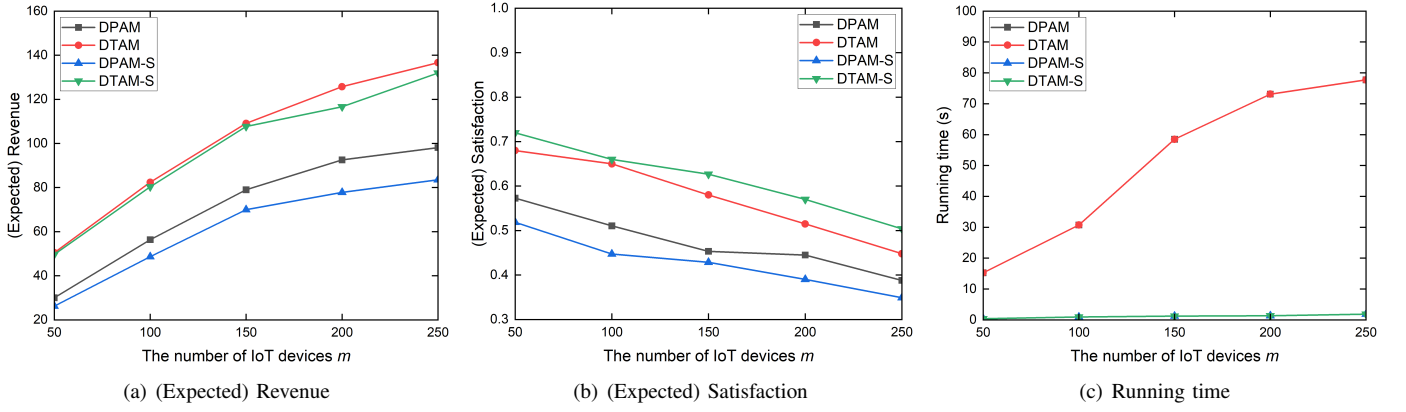


Fig. 4. The performances of proposed mechanisms on different number of edge nodes, where  $n = 50$ ,  $k = 3$ ,  $\sigma = 0.1$ , and  $\varepsilon = 200$ .

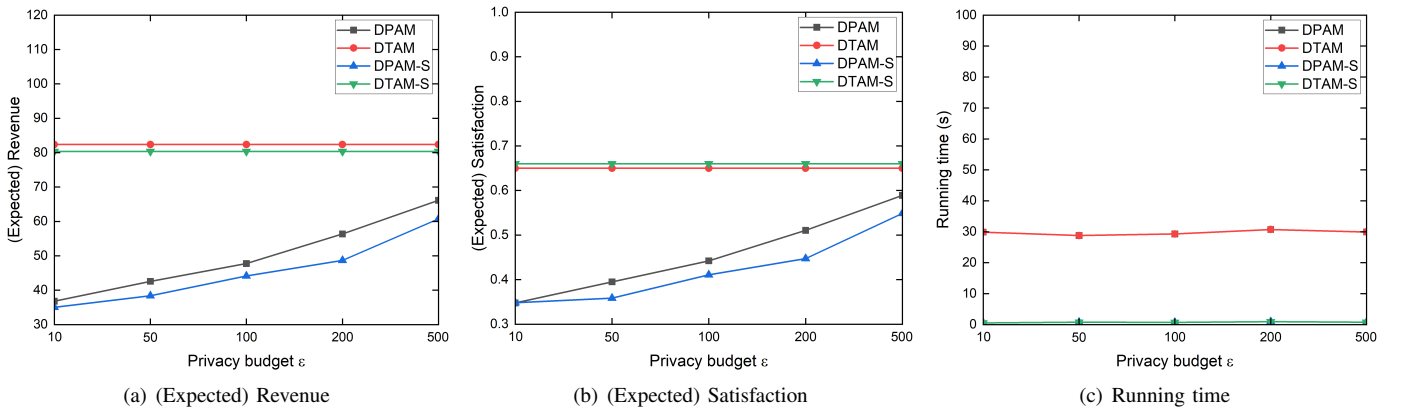


Fig. 5. The performances of proposed mechanisms on different privacy budgets, where  $m = 100$ ,  $n = 50$ ,  $k = 3$ , and  $\sigma = 0.1$ .

revenue and satisfaction show upward trends with the increase of privacy budget. Actually, the privacy budget controls the degree of protection provided by differential privacy. The higher the privacy budget, the higher the revenue and satisfaction, but the degree of privacy protection will be weakened. Shown as Figure 5 (c), the running time remains the same with the increase of privacy budget, which indicates that the running time has no concern with the choice of privacy budget.

Based on the above four tasks, the main conclusions can be summarized as follows. The granularity affects the running time significantly, and it is usually not necessary to choose a very small granularity to ensure accuracy. In the case of a large number of resource types, the DPAM (DTAM) is not applicable due to the limitation of time complexity. Under the condition of sufficient network bandwidth, the more participating IoT devices, the better the revenue. We need to balance the contradiction between privacy protection and revenue by choosing a privacy budget.

## VII. CONCLUSION

In this paper, we propose an edge-thing system based on blockchain technology and smart contract, which achieves complete decentralization and tampering-proof. In order to model the resources allocation and pricing between IoT devices and edge nodes, we formulate a novel combinatorial

double auction problem. Then, we introduce differential privacy into the auction so as to prevent privacy leakage further. First, we design the DPAM mechanism, and prove it satisfies  $\varepsilon$ -differential privacy,  $\gamma$ -truthfulness, individual rationality, budget balance, but not computational efficiency. It is not suitable to use in the case of too many resource types. Then, we propose the DPAM-S mechanism to reduce the time complexity to polynomial time, and satisfy the above desired properties as well. Finally, we built a virtual region to test our proposed mechanisms by extensive simulations, which confirms our theoretical analysis.

## ACKNOWLEDGMENT

This work is supported by Guangdong Key Lab of AI and Multi-modal Data Processing, National Natural Science Foundation of China (NSFC) Project No. 61872239; BNU-UIC Institute of Artificial Intelligence and Future Networks funded by Beijing Normal University at Zhuhai (BNU Zhuhai) and AI-DS Research Hub, BNU-HKBU United International College (UIC), Zhuhai, Guangdong, China.

## REFERENCES

- [1] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for internet of things applications: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601–628, 2017.

- [2] A. A. Alli and M. M. Alam, "Secoff-fciot: Machine learning based secure offloading in fog-cloud of things for smart city applications," *Internet of Things*, vol. 7, p. 100070, 2019.
- [3] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2016.
- [4] J. Guo, X. Ding, and W. Wu, "A blockchain-enabled ecosystem for distributed electricity trading in smart city," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 2040–2050, 2020.
- [5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.
- [6] R. Zhu, Z. Li, F. Wu, K. Shin, and G. Chen, "Differentially private spectrum auction with approximate revenue maximization," in *Proceedings of the 15th ACM international symposium on mobile ad hoc networking and computing*, 2014, pp. 185–194.
- [7] R. Zhu and K. G. Shin, "Differentially private and strategy-proof spectrum auction with approximate revenue maximization," in *2015 IEEE conference on computer communications (INFOCOM)*. IEEE, 2015, pp. 918–926.
- [8] C. Dwork, "Differential privacy: A survey of results," in *International conference on theory and applications of models of computation*. Springer, 2008, pp. 1–19.
- [9] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*. IEEE, 2007, pp. 94–103.
- [10] H. Jin, L. Su, B. Ding, K. Nahrstedt, and N. Borisov, "Enabling privacy-preserving incentives for mobile crowd sensing systems," in *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2016, pp. 344–353.
- [11] J. Lin, D. Yang, M. Li, J. Xu, and G. Xue, "Bidguard: A framework for privacy-preserving crowdsensing incentive mechanisms," in *2016 IEEE conference on communications and network security (CNS)*. IEEE, 2016, pp. 145–153.
- [12] J. Guo and W. Wu, "Differential privacy-based online allocations towards integrating blockchain and edge computing," *arXiv preprint arXiv:2101.02834*, 2021.
- [13] T. Ni, Z. Chen, L. Chen, S. Zhang, Y. Xu, and H. Zhong, "Differentially private combinatorial cloud auction," *IEEE Transactions on Cloud Computing*, pp. 1–1, 2021.
- [14] D. Yang, G. Xue, X. Fang, and J. Tang, "Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones," *IEEE/ACM transactions on networking*, vol. 24, no. 3, pp. 1732–1744, 2015.
- [15] J. Guo, X. Ding, and W. Wu, "Reliable traffic monitoring mechanisms based on blockchain in vehicular networks," *IEEE Transactions on Reliability*, pp. 1–1, 2021.
- [16] W. Wang, B. Liang, and B. Li, "Designing truthful spectrum double auctions with local markets," *IEEE Transactions on Mobile Computing*, vol. 13, no. 1, pp. 75–88, 2012.
- [17] A. Yassine, M. S. Hossain, G. Muhammad, and M. Guizani, "Double auction mechanisms for dynamic autonomous electric vehicles energy trading," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 8, pp. 7466–7476, 2019.
- [18] W. Sun, J. Liu, Y. Yue, and H. Zhang, "Double auction-based resource allocation for mobile edge computing in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4692–4701, 2018.
- [19] U. Habiba, S. Maghsudi, and E. Hossain, "A reverse auction model for efficient resource allocation in mobile edge computation offloading," in *2019 IEEE global communications conference (GLOBECOM)*. IEEE, 2019, pp. 1–6.
- [20] X. Peng, K. Ota, and M. Dong, "Multiattribute-based double auction toward resource allocation in vehicular fog computing," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3094–3103, 2020.
- [21] W. Sun, J. Liu, Y. Yue, and P. Wang, "Joint resource allocation and incentive design for blockchain-based mobile edge computing," *IEEE Transactions on Wireless Communications*, vol. 19, no. 9, pp. 6050–6064, 2020.
- [22] Y. Jiao, P. Wang, D. Niyato, and K. Suankaewmanee, "Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 9, pp. 1975–1989, 2019.
- [23] X. Ding, J. Guo, D. Li, and W. Wu, "An incentive mechanism for building a secure blockchain-based internet of things," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 1, pp. 477–487, 2020.
- [24] —, "Pricing and budget allocation for iot blockchain with edge computing," *arXiv preprint arXiv:2008.09724*, 2020.
- [25] J. Guo, X. Ding, and W. Wu, "A double auction for charging scheduling among vehicles using dag-blockchains," *arXiv preprint arXiv:2010.01436*, 2020.
- [26] Z. Chen, T. Ni, H. Zhong, S. Zhang, and J. Cui, "Differentially private double spectrum auction with approximate social welfare maximization," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 11, pp. 2805–2818, 2019.
- [27] Q. Xiang, L. Kong, X. Liu, J. Xu, and W. Wang, "Auc2reserve: A differentially private auction for electric vehicle fast charging reservation," in *2016 IEEE 22nd International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA)*. IEEE, 2016, pp. 85–94.
- [28] D. Li, Q. Yang, W. Yu, D. An, Y. Zhang, and W. Zhao, "Towards differential privacy-based online double auction for smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 971–986, 2019.
- [29] G. Gao, M. Xiao, J. Wu, S. Zhang, L. Huang, and G. Xiao, "Dpdt: A differentially private crowd-sensed data trading mechanism," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 751–762, 2019.
- [30] A. Gupta, K. Ligett, F. McSherry, A. Roth, and K. Talwar, "Differentially private combinatorial optimization," in *Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete Algorithms*. SIAM, 2010, pp. 1106–1125.
- [31] Y. S. Son, R. Baldick, K.-H. Lee, and S. Siddiqi, "Short-term electricity market auction game analysis: uniform and pay-as-bid pricing," *IEEE Transactions on Power Systems*, vol. 19, no. 4, pp. 1990–1998, 2004.



**Jianxiong Guo** received his Ph.D. degree from the Department of Computer Science, University of Texas at Dallas, Richardson, TX, USA, in 2021, and his B.E. degree from the School of Chemistry and Chemical Engineering, South China University of Technology, Guangzhou, Guangdong, China, in 2015. He is currently an Assistant Professor with the BNU-UIC Institute of Artificial Intelligence and Future Networks, Beijing Normal University at Zhuhai, and also with the Guangdong Key Lab of AI and Multi-Modal Data Processing, BNU-HKBU United International College, Zhuhai, Guangdong, China. His research interests include social networks, algorithm design, data mining, IoT application, blockchain, and combinatorial optimization.



**Xingjian Ding** received his B.E. degree in electronic information engineering from Sichuan University in 2012 and M.S. degree in software engineering from Beijing Forestry University in 2017. He obtained his Ph.D. degree from the School of Information, Renmin University of China in 2021. He is currently an assistant professor at the School of Software Engineering, Beijing University of Technology. His research interests include wireless rechargeable sensor networks, approximation algorithms design and analysis, and blockchain.



**Weijia Jia** is currently a Chair Professor and Director of BNU-UIC Institute of Artificial Intelligence and Future Networks, Beijing Normal University at Zhuhai; VP for Research of BNU-HKBU United International College. His contributions have been recognized as optimal network routing and deployment, anycast and QoS routing, sensors networking, AI (knowledge relation extractions; NLP etc.) and edge computing. He has over 600 publications in the prestige international journals/conferences and research books and book chapters. He is the Fellow of IEEE and the Distinguished Member of CCF.