Computers, Materials & Continua
DOI: 10.32604/cmc.2023.034770
Article

Tech Science Press

A Dynamic Multi-Attribute Resource Bidding Mechanism with Privacy Protection in Edge Computing

Shujuan Tian[1,2,3], Wenjian Ding[1,2,3], Gang Liu[4], Yuxia Sun[5], Saiqin Long[5] and Jiang Zhu[1,2,3,*]

[1]Xiangtan University, Xiangtan, 411105, China
[2]Key Laboratory of Hunan Province for Internet of Things and Information Security, Xiangtan, 411105, China
[3]Hunan International Scientific and Technological Cooperation Base of Intelligent Network, Xiangtan,411105, China
[4]Hunan University, Changsha, 410082, China
[5]Jinan University, Guangzhou, 510632, China
*Corresponding Author: Jiang Zhu. Email: zhu_jiang@xtu.edu.cn
Received: 27 July 2022; Accepted: 09 November 2022

Abstract: In edge computing, a reasonable edge resource bidding mechanism can enable edge providers and users to obtain benefits in a relatively fair fashion. To maximize such benefits, this paper proposes a dynamic multi-attribute resource bidding mechanism (DMRBM). Most of the previous work mainly relies on a third-party agent to exchange information to gain optimal benefits. It is worth noting that when edge providers and users trade with third-party agents which are not entirely reliable and trustworthy, their sensitive information is prone to be leaked. Moreover, the privacy protection of edge providers and users must be considered in the dynamic pricing/transaction process, which is also very challenging. Therefore, this paper first adopts a privacy protection algorithm to prevent sensitive information from leakage. On the premise that the sensitive data of both edge providers and users are protected, the prices of providers fluctuate within a certain range. Then, users can choose appropriate edge providers by the price-performance ratio (PPR) standard and the reward of lower price (LPR) standard according to their demands. The two standards can be evolved by two evaluation functions. Furthermore, this paper employs an approximate computing method to get an approximate solution of DMRBM in polynomial time. Specifically, this paper models the bidding process as a non-cooperative game and obtains the approximate optimal solution based on two standards according to the game theory. Through the extensive experiments, this paper demonstrates that the DMRBM satisfies the individual rationality, budget balance, and privacy protection and it can also increase the task offloading rate and the system benefits.

Keywords: Edge computing; approximate computing; nash equilibrium; privacy protection

1 Introduction

With the development of the Internet of Things (IoT), computation-intensive applications (e.g., virtual reality, face recognition, and online games) are developing rapidly. The continuous improvement of quality of service (QoS) for users and the development of related applications have resulted in high computing performance and low latency requirements for the IoT [1]. Edge computing is a distributed architecture that is close to users and therefore provides faster service than cloud computing [2]. Edge providers are rich in resources with low latency and widely rented by IoT users [3]. Therefore, how to rent edge resources at a reasonable price has become a computational economic problem [4].

Resource bidding is the first problem to be resolved in the edge resource transaction. Generally, multiple providers are competitive, because edge users can choose various combinations of edge providers according to different edge resource attributes. For edge providers, the benefits are determined by the bidding price and the number of edge resources that are traded. For edge users, their benefits are related to their tasks with different complexity, size, and latency [5]. Hence, how to price reasonably to maximize the benefits for edge users and providers is challenging. The bidding problem of edge providers is similar to the bin packing problem [6], which is NP-hard and cannot get an optimal solution in polynomial time. So, the edge resource transaction between multiple providers and users can be regarded as a typical non-cooperative game [7]. A price equilibrium point lies in the non-cooperative game model to maximize the benefits for edge providers and users.

Another important issue to be aware of in edge resource transactions is the potential disclosure of commercially sensitive information, such as provider costs and previous transaction data. The transaction information of edge resources is collected by third-party agents that are reliable and won't leak the participants' private information [8,9]. However, these agents are honest-but-curious about their users [10]. They may snoop on the privacy of transaction participants and might obtain such private information. Most of the existing privacy protection models used by third-party agents for data publishing are vulnerable to attacks [11,12]. Therefore, it is necessary to establish a new secure edge resource bidding system to effectively combine information protection and benefit optimization in the resource transaction process.

To overcome the above issues, this paper constructs a secure edge resource bidding mechanism named Dynamic Multi-attribute Resources Bidding Mechanism (DMRBM). It not only protects the sensitive information of edge users and providers, but also helps edge providers price appropriately. As a result, both edge providers and users can maximize the benefits while meeting the users' needs.

The DMRBM consists of a privacy protection part and a dynamic multi-attribute edge resource bidding part. On the one hand, the privacy protection part combines sampling [13] and differential privacy [14] to protect the information of edge providers and users. Compared to the existing resource bidding mechanism [8,15], our proposed mechanism reduces the computational complexity with the sampling strategy, and improves the privacy protection level as well as the performance with the differential privacy strategy. On the other hand, on the premise that the sensitive data of both providers and users are protected, the prices of providers fluctuate within a certain range. Therefore, a dynamic pricing strategy for multi-attribute resources is proposed in this paper. First, in order to normalize the QoS of providers, multi-attribute values are mapped into the same dimension and combined these values according to the user's preferences. Second, since the price of one edge provider changes dynamically with the prices of users and other edge providers, two evaluation functions are proposed, i.e., PPR and LPR. These two evaluation functions maximize for users and edge providers by selecting appropriate edge providers in resource transactions. Then, the users combine the results of two evaluation functions by a weighted method, according to their preferences. Finally, the approximate optimal solution is calculated based on the game theory [16,17].

Our main contributions are listed as follows:

- Based on the dynamic characteristics of prices of different edge providers and different user demands, a dynamic multi-attribute edge resource bidding mechanism is designed to achieve reasonable prices. Furthermore, this paper approximately computes the maximum benefits based on game theory by conducting the evaluation functions of providers, including PPR and LPR.
- Differential privacy method is used to prevent information leaks. The average benefits of the privacy protection mechanism are 12% higher than that without the protection mechanism.
- Non-cooperative game is constructed between providers and users. It proves that the generated prices sequence from our resource bidding mechanism is convergent and it approaches the Nash equilibrium solution.

The rest of the paper is organized as follows. Section 2 introduces some related work. Section 3 analyzes the system model and the problem that should be solved. Section 4 designs the details of the proposed DMRBM. In Section 5, we list extensive experiments and make comparisons. Finally, our conclusions are discussed in Section 6.

2 Related Work

We make a brief summary and analysis of the work related to two topics: (1) the edge computing resource bidding; (2) the security issues in edge computing.

As for resource bidding, there are many game models to get the maximum benefits for both edge providers and users, such as Bilateral market game [18,19], Stackelberg game [20], Maximize game [21], etc. When it comes to competitions, the models can be divided into the following three categories. Zhang et al. [20] used a multi-provider single user model, aiming at increasing the demand and the benefit for a single user, and multiple providers bid to achieve a price equilibrium. Begam et al. [22] considered a multi-user pricing model for revenue generation. In view of the inappropriate behaviors in bidding, Xie et al. [19] employed a method of increasing the punitive function to adjust the price, so as to improve the fairness and trustworthiness of the game. Guo et al. [23] proposed a novel trust evaluation method by integrating the comparison of true utility and expected utility in auction mechanism. However, a common shortcoming of the aforementioned work is that they failed to cope with the information security issue, e.g., price protection by edge providers and information leaks by a third-party agent. Therefore, these models remain vulnerable to opponents. From a practical point of view, it is increasingly insecure about releasing real information.

The information security problem attracts many researchers. Some encryption algorithms are indeed very popular in the field of information security. You et al. [24] made a summary of some common security protection models. Ram et al. [25] protected data through data encryption and distribution. Gu et al. [26] studied the privacy of data transmission between multi-edge nodes and end-users. But in the field of big data, encryption and decryption methods face long delays. Their computational complexity cannot meet the demand of real-time performance. Approximate computing can reduce design complications with an increase in performance and efficiency for error-resilient applications [27]. A trust-based multi-agent imitation learning (T-MAIL) scheme was proposed in [28]. To avoid encryption/decryption delays, an approximate computing method was introduced [29]. Lei et al. [30] used approximate dynamic programming techniques to solve joint computing offload and multi-user scheduling problems. Derbeko et al. [31] suggested the sampling of an approximate computing as a method of improving computational performance. Wang et al. [32] proposed a novel verifiable multi-dimensional (t,n) threshold quantum state sharing scheme to overcome the shadow attack.

Apart from encryption algorithms, other approaches are explored in the field of information security. Blockchain technology can be used for privacy protection in [33]. Huo et al. [34] summarized the privacy issues in a cloud/edge-based industrial IoT system. An efficient and privacy-protected VANETs data offload scheme based on the concept of edge computing is proposed in [35]. They explored certain approaches to ensure information security in the process of edge resource reservation. But they failed to take the numerical characteristics of information into consideration and the operation was complicated. A mechanism is heuristically introduced to ensure information security by differential privacy [36].

3 System Model and Problem Formulation

In this section, the entities of the resource bidding system in edge computing are initially described. Then, this paper analyzes the way of bidding information leakage in edge computing. Finally, this paper integrates the optimization objectives of edge resource bidding.

3.1 System Model

The edge providers have many types of resources and each provider's resource capacity is limited. Since the user requirements tend to be met by multiple edge providers, to simplify the model complexity, this paper first considers the system with only transactions among a single user and multiple providers.

Edge Providers: The resource attributes are represented by matrix $\boldsymbol{K}$:

$$\boldsymbol{K} = \begin{bmatrix} k_{1,1} & \cdots & k_{1,K} \\ \vdots & \ddots & \vdots \\ k_{n,1} & \cdots & k_{n,K} \end{bmatrix} \tag{1}$$

n denotes the total number of providers and K represents the total number of the edge resources' attributes. This paper assumes that $\boldsymbol{p} = \{p_1, \cdots, p_n, \cdots, p_N\}$, where p_n represents the n-th edge provider's initial prices. $\boldsymbol{h} = \{h_1, \cdots, h_n, \cdots, h_N\}$ is regarded as the costs of all edge providers, where h_n stands for the cost of n-th edge provider. It is easy to know that the prices must be higher than the costs of edge providers, i.e., $p_n \geq h_n, \forall n \in N$. $\boldsymbol{Q} = \{Q_1, \cdots, Q_n, \cdots, Q_N\}$ refers to the QoS of the edge providers.

Aggregator: Each aggregator corresponds to a single user and E edge providers. The process in the aggregator is as follows. First, the edge providers deliver their information (e.g., price, QoS, and cost) into the aggregator. Second, these providers compete in the aggregator in the non-cooperation game theory. Then the aggregator will choose the appropriate providers aiming to maximize the benefits for the user and the providers when these providers meet the user's requirements. Finally, the aggregator returns the competition results to the user and providers.

User: The user chooses edge resources from N providers, considering K attributes of the resources. $\overline{p}, t$ and Z represent the maximum acceptable prices for the user and the user's benefits when it has accomplished its jobs and its QoS demand, respectively. The user can purchase multiple attributes of multiple edge providers in combination.

Fig. 1 depicts a user's resource combination process based on multiple edge providers. Each provider has different resources in practice. For the convenience of drawing and describing, this paper supposes that each provider has only one unique resource, e.g., the edge provider EP_1 has a unique resource S_1. Depending on whether the provider is selected or not, there are 256 ways to combine providers' resources, and the user chooses the most beneficial one. For example, there are 5 selected edge providers, each provider has 3 different attribute resources, different costs, and different prices. The user will choose the combination of edge providers to meet its requirement and keep costs as low as possible. It may cause privacy leakage in the bidding process of edge resources. For example, when the aggregators make requests to edge providers and users, the edge providers and users can be attacked, resulting in privacy leakages. Besides, the aggregators receive responses from edge providers and users, and may share information about edge providers and users with other users or aggregators for monetary purposes (e.g., advertising). Similarity attacks and knowledge background attacks are often encountered in bidding. The attackers can infer the private information that can affect the result of resource bidding through unimportant information.

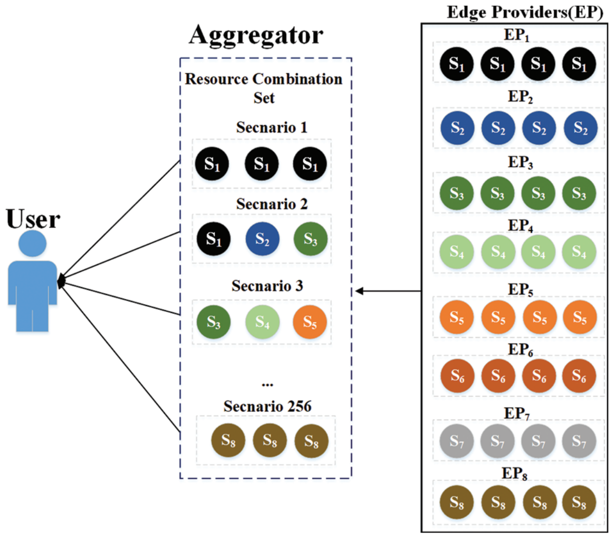


Figure 1: Combination process of multiple edge providers' resources

3.2 Problem Formulation

The total benefits for the user are determined by the benefits from completing tasks and the cost of purchasing resources from edge providers. So, this paper detects the total benefits for the user by:

$$U = t - \sum_{n=1}^{N} y_n W_n p_n^* \tag{2}$$

where y_n, W_n and p_n^* respectively represent the decision of whether the EP_n is purchased by the user, the QoS which is provided by EP_n and the optimal price of EP_n when it is purchased by the user.

The benefit for the edge provider EP_n is defined as:

$$\pi_n = y_n W_n (p_n^* - h_n) \tag{3}$$

The optimization objectives could be expressed as:

$$
\begin{aligned}
&max\ U \\
&max\ \pi_n, \forall n \\
&\text{s.t. } C1\text{: } p_n^* > h_n \\
&C2\text{: } W_n \le Q_n \\
&C3\text{: } y_n \in \{0, 1\}
\end{aligned}
\tag{4}
$$

The restrictions C1, C2, and C3 represent the price restriction, the resource restriction, and the decision restriction, respectively.

4 Algorithm Design

In this section, this paper considers the whole process of creating a fair resource bidding mechanism with privacy protection. Since it is NP-hard to directly solve the maximum benefit problem, the approximate maximum benefit for edge providers and the user is calculated by approximate computing. This paper first designs a DMRBM based on a game theory in ***4.1***. It is noticed that when edge providers and users trade with third-party agents, their sensitive information is easy to be leaked. Therefore, in the bidding mechanism, this paper adopts the privacy protection algorithm which is composed of sampling and differential privacy to prevent sensitive information leakage caused by third-party agents. The privacy protection algorithm is depicted in ***4.2***.

The architecture of DMRBM is shown in Fig. 2. First, this paper calculates the QoS of edge providers through expert preference. Afterward, this paper designs a privacy protection algorithm. Next, the initial provider combination is selected according to the user's preference for resource attributes. Each provider adjusts the optimal price through the non-cooperative game. Finally, when all the prices of providers tend to be stable, the user makes the final purchase decision and the providers set the prices according to the purchase decision.

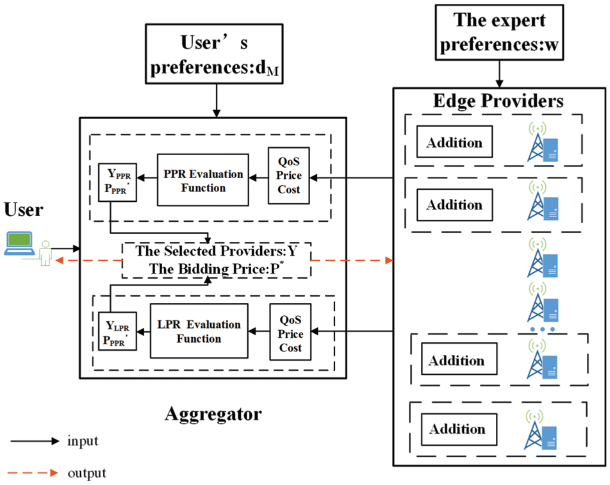


Figure 2: Architecture of DMRBM

4.1 Dynamic Multi-Attribute Resource Bidding Mechanism

The QoS value of the edge provided to the user is determined by the values and the expert preference of multiple attributes. This paper normalizes the attributes using feature scaling, and all the values lie into [0,M]:

$$k'_{i,j} = M \cdot \frac{k_{i,j} - min\{k_{\cdot,j}\}}{max\{k_{\cdot,j}\} - min\{k_{\cdot,j}\}} \tag{5}$$

$min\{k_{\cdot,j}\}$ and $max\{k_{\cdot,j}\}$ are minimum and maximum of all providers' j-th attribute values, respectively. This paper uses simple addition weighting (SAW) [37] to perform the comparison of quality attributes. The QoS that the provider EP_n can provide to the user is:

$$Q_n = \sum\nolimits_{k \in K} \omega_k \cdot k'_{n,k} \tag{6}$$

$\boldsymbol{\omega} = (\omega_1, \cdots, \omega_K)$ is a K-dimension vector of the attribute preferences for edge resources. This vector meets the condition that $\sum\nolimits_{k \in K} \omega_k = 1, \omega_k \in [0, 1]$.

To select providers effectively and reasonably, while maximizing the benefits for both providers and the user, the following two evaluation functions are introduced: (1) Price-Performance Ratio (PPR) evaluation function; (2) Lower Price based on Rewards (LPR) evaluation function. It is apparent that choosing the edge provider with the highest cost performance ratio (i.e., PPR) for transaction will bring maximum benefits for the user. To maintain a reasonable and fair competition environment for resources, a better solution is to combine multiple edge providers to conduct transactions while maintaining benefits. Therefore, LPR is proposed for edge providers. First, this paper assumes that the user has a preference $d_M = \langle i, j \rangle$, i and j respectively indicating the probability that the user chooses the providers based on the PPR and LPR. Meanwhile, $i + j = 1$. The PPR and LPR evaluation functions are defined as:

$$PPR_e = \frac{Q_e}{p_e} \tag{7}$$

$$LPR_e = \mu \frac{1}{p_e} + (1 - \mu) re_e, \mu \in (0, 1) \tag{8}$$

where re_e represents the reward given by the system and is determined by the PPR of all selected providers. In detail, re_n is directly proportional to its PPR. Thus, the reward of provider n is:

$$re_n = \frac{Re \cdot PPR_n}{\sum\nolimits_{e=1}^{N} PPR_e} \tag{9}$$

where Re is the total reward given by the system. The two evaluation functions evaluate providers from different perspectives, and they are also correlated. The LPR evaluation function focuses on selecting edge providers with a low price but relatively high PPR. The higher the PPR evaluation function value of edge provider n is, the higher the reward re_n will be. The higher PPR or LPR is, the more likely the provider will be selected. After determining the evaluation functions, the providers should enhance their competitiveness by adjusting their prices. Here this paper elaborates form the perspective of game theory.

There are E players in the game and each participating provider can be seen as a player. Each player has three elements, i.e., price, QoS, and cost. $\boldsymbol{p}'_{\boldsymbol{E}} = \{p'_1, \cdots, p'_e, \cdots, p'_E\}$, $\boldsymbol{Q}'_{\boldsymbol{E}} = \{Q'_1, \cdots Q'_e, \cdots, Q'_E\}$ and $\boldsymbol{h}'_{\boldsymbol{E}} = \{h'_1, \cdots, h'_e, \cdots, h'_E\}$ respectively refer to the prices, QoS and costs of all participating providers. Furthermore, this paper lets $\boldsymbol{Y}^{\boldsymbol{r_1}} = \{Y_1^{r1}, \cdots, Y_E^{r1}\}$ and $\boldsymbol{Y}^{\boldsymbol{r_2}} = \{Y_1^{r2}, \cdots, Y_E^{r2}\}$, where Y_1^{r1} and $Y_1^{r2} \in \{0, 1\}$. They indicate the decision sets in the r_1-th round and r_2-th round of the providers in PPR and LPR respectively. In the two functions, $p^{*}_{PPR,e}$ and $p^{*}_{LPR,e}$ mean two final prices of providers EP_e. If $Y^{r_1}_1 = 0$ and $Y^{r_2}_1 = 0$, the provider EP_e does not provide any resources to the user. Otherwise, the provider can provide resources to the user. The game runs by the following steps:

Step 1: Initialize the game. Initialize the price p'_e, QoS Q'_e, the cost h'_e by Algorithm 2 for privacy protection and set the initial $Y^0_e = 1$ for each provider EP_e.

Step 2: Calculate the critical price. Calculate the PPR value by Eq. (7). The critical price is the optimal price for providers in the current state and it refers to the price at which a provider can get the maximum benefit when the price and QoS of other providers are determined. If the price performance of the provider is at an average level of the price performance of all alternative providers, the price of the provider is at a critical price. The provider EP_e adjusts the price according to the average PPR value of other providers. Then, the critical value $p^{r_1}_{PPR,e}$ for PPR function in the r_1-th round of EP_e is defined by:

$$p^{r_1}_{PPR,e} = \begin{cases} \overline{p}, p^{r_1}_{PPR,e} > \overline{p} \\ \dfrac{|\boldsymbol{Y}^{r_1-1} \backslash \{e\}| Q'_e}{\sum_{y \epsilon \boldsymbol{Y}^{r_1-1} \backslash \{e\}} PPR_y}, h'_e \le p^{r_1}_{PPR,e} \le \overline{p} \\ 0, Y^{r_1}_e = 0 \end{cases} \tag{10}$$

If $p^{r_1}_{PPR,e} > \overline{p}$ or $h'_e > p^{r_1}_{PPR,e}$, EP_e will be withdrawn from the PPR game and $Y^{r_1}_e = 0$. If not, $Y^{r_1}_e = 1$. For example, there are 5 edge providers, these providers' QoS, prices, and costs are $\boldsymbol{Q}$' $= \{10, 20, 25, 30, 15\}$, $\boldsymbol{p}$' $= \{10, 10, 20, 10, 20\}$, $\boldsymbol{h}$' $= \{5, 3, 10, 20, 8\}$. This paper calculates the critical price $p^{1}_{PPR,1}$ in the first round. The average PPR of other providers $\dfrac{\sum_{e \in \{2,3,4,5\}} PPR_e}{4} = 1.75$. Thus, $p^{1}_{PPR,1} = \dfrac{Q'_1}{1.75} = 5.71$. Due to $p^{1}_{PPR,1} > h'_1$, this paper considers the critical price to be feasible.

Since the reward re_e can be fixed according to PPR_e, this paper regards the reward as a fixed amount. If the price of a provider is at an average level of the prices of all optional providers, the price of this provider is also at a critical price. To reasonably improve the LPR value and get more benefits, EP_e alters the price $p^{r_2}_{LPR,e}$ based on the prices of other providers. Calculate the critical price $p^{r_2}_{LPR,e}$ by:

$$p^{r_2}_{PPR,e} = \begin{cases} \overline{p}, p^{r_2}_{PPR,e} > \overline{p} \\ \dfrac{\sum_{y \in \boldsymbol{Y}^{r_2-1} \backslash \{e\}} p^{r_2-1'}_{LPR,y}}{|\boldsymbol{Y}^{r_2-1} \backslash \{e\}|}, h'_e - re_e \le p^{r_2}_{LPR,e} \le \overline{p} \\ 0, Y^{r_2}_e = 0 \end{cases} \tag{11}$$

If the price $h'_e - re_e > p^{r_2}_{LPR,e}$ or $p^{r_2}_{LPR,e} > \overline{p}$, the player EP_e will be withdrawn from the game and $Y^{r_2}_e = 0$. In neither cases, $Y^{r_2}_e = 1$.

Step 3: Make the final price and strategy. Compute all the players' prices iteratively. This process will not end until the prices $p^{r_1}_{PPR,e}$ and $p^{r_2}_{PPR,e}$ no longer change with each EP_e and the players no longer change in the nearest two iterations. In each iteration, compute the critical price by Eqs. (10) and (11) separately. The iteration will end when $\boldsymbol{Y}^{r_1} = \boldsymbol{Y}^{r_1-1}$, $||\boldsymbol{p}^{r_1}_Y - \boldsymbol{p}^{r_1-1}_Y|| \le G$, $\boldsymbol{Y}^{r_2} = \boldsymbol{Y}^{r_2-1}$ and $||\boldsymbol{p}^{r_2}_Y - \boldsymbol{p}^{r_2-1}_Y|| \le G$ are met. The solutions $p^{r_1}_{PPR,e}$ and $p^{r_2}_{LPR,e}$ are unique, and the user can choose multiple providers to purchase resources and complete the tasks.

After circling the three steps, the aggregator will get the results $\boldsymbol{Y^{r_1}}$, $\boldsymbol{Y^{r_2}}$, $\boldsymbol{p^*_{PPR}}$ and $\boldsymbol{p^*_{LPR}}$. In the bidding process, this paper comes up with a method to calculate the proper price p^*_E, as the combination of $p^*_{PPR,e}$ and $p^*_{LPR,e}$ for EP_e. A final decision profile $\boldsymbol{Y} = \{Y_1, \cdots, Y_E\}$ for the user is defined as:

$$Y_e = \begin{cases} 1, & Y_e^{r_1} = 1 \ or \ Y_e^{r_2} = 1 \\ 0, & otherwise \end{cases} \tag{12}$$

where W_e is composed of $W_{PPR,e}$ and $W_{LPR,e}$. They represent QoS transactions between the user and the provider EP_e based on PPR and LPR. $W_{PPR,e}$ and $W_{LPR,e}$ are defined as:

$$\begin{aligned} W_{PPR,e} &= \frac{Y_e^{r_1} Q'_e Z}{p^*_{PPR,e} \sum_{y \in \boldsymbol{Y^{r_1}}} PPR_y} \cdot i \\ W_{LPR,e} &= \frac{Y_e^{r_2} Q'_e Z}{P^*_{LPR,e} \sum_{y \in \boldsymbol{Y^{r_2}}} PPR_y} \cdot j \end{aligned} \tag{13}$$

where Z means the user's QoS demand. Since the strategy $\boldsymbol{Y}$ has been determined, this paper can measure the synthetical prices of the providers with the user's preference by:

$$p^*_e = \begin{cases} i \cdot p^*_{PPR,e} + j \cdot p^*_{LPR,e}, & Y_e = 1 \\ 0, & otherwise \end{cases} \tag{14}$$

where i and j indicate the probability that the user chooses the providers based on PPR and LPR. The total benefits of the player EP_e are composed of $\pi_{\left(Y_e^{r_1}, \boldsymbol{Y^{r_1}_{(-e)}}\right)}$ and $\pi_{\left(Y_e^{r_2}, \boldsymbol{Y^{r_2}_{(-e)}}\right)}$, which represents the benefits of the two evaluation functions respectively. The benefits of the two evaluation functions are denoted as:

$$\begin{aligned} \pi_{\left(Y_e^{r_1}, \boldsymbol{Y^{r_1}_{(-e)}}\right)} &= W_{PPR,e} \left(p^*_{PPR,e} - h'_e\right) \\ \pi_{(Y_e^{r_2}, \boldsymbol{Y^{r_2}_{(-e)}})} &= W_{LPR,e}(p^*_{PPR,e} - h'_e + re_e) \end{aligned} \tag{15}$$

Algorithm 1: Dynamic multi-attribute resource bidding mechanism (DMRBM)

```
Input: $N, K_N, I^*_K, \omega_K, s, p, \lambda, \overline{p}$, and $G$
Output: $p^*_E$, $W_E, \pi_E$, and $U$
$r_1 = 0, r_2 = 0$;
calculate the $p'_E$, $Q'_E$, $h'_E$, $\boldsymbol{Y}$ by Algorithm 2;
$\boldsymbol{Y^{r_1}} = \boldsymbol{Y}, \boldsymbol{Y^{r_2}} = \boldsymbol{Y}$;
for edge provider $e \in E$ do
    $p^{r_1}_{PPR,e} = p'_e, p^{r_2}_{LPR,e} = p'_e$;
    if edge provider $e \in \boldsymbol{Y^{r_1}}$ then
        calculate $p^{r_1+1}_{PPR,e}$ by Eq. (10);
        if ($p^{r_1+1}_{PPR,e} < h'_e$) then
            $p^{r_1+1}_{PPR,e} = 0$, $Y_e^{r_1} = 0$;
        end if
```

(Continued)

Algorithm 1: Continued

```
12:     **else if** edge provider $e \in \boldsymbol{Y}^{r_2}$ then
13:         calculate $re_e, p_{LPR,e}^{r_2+1}$ respectively by Eqs. (9) and (11);
14:         **if** ($p_{LPR,e}^{r_2+1} < h_e - re_e$) then
15:             $p_{LPR,e}^{r_2+1} = 0,\ Y_e^{r_2} = 0$;
16:         **end if**
17:     **end if**
18: **end for**
19: $r_1 = r_1 + 1, r_2 = r_2 + 1$;
20: **if** ($\boldsymbol{Y}^{r_1} \neq \boldsymbol{Y}^{r_1-1} or\ ||\boldsymbol{p}_{\boldsymbol{Y}^{r_1}} - \boldsymbol{p}_{\boldsymbol{Y}^{r_1-1}}|| > G$) then
21:     repeat step 7 to 11;
22: **end if**
23: **if** ($\boldsymbol{Y}^{r_2} \neq \boldsymbol{Y}^{r_2-1} or\ ||\boldsymbol{p}_{\boldsymbol{Y}^{r_2}} - \boldsymbol{p}_{\boldsymbol{Y}^{r_2-1}}|| > G$) then
24:     repeat step 13 to 15;
25: **end if**
26: update $\boldsymbol{Y}$ by Eq. (12);
27: **for** edge provider $e \in \boldsymbol{Y}$ **do**
28:     $p_{PPR,e}^{*} = p_{PPR,e}^{r_1}; p_{LPR,e}^{*} = p_{LPR,e}^{r_2}$;
29:     calculate $W_{PPR,e}, W_{LPR,e}$ by Eq. (13);
30:     calculate $p_e^{*}, \pi_e$ respectively by Eqs. (14) and (15);
31: **end for**
32: calculate $U$ by Eq. (2);
33: return $p_E^{*}, W_E, \pi_E, U$
```

This paper designs Algorithm 1 to solve the resource transaction problem in dynamic multi-attribute resource bidding. In this algorithm, the critical prices p_{PPR}^{*} and p_{LPR}^{*} are first calculated based on the game theory. Then, the decision $\boldsymbol{Y}$, W_e and the benefits can also be calculated. The original data of edge providers and the user in Algorithm 1 is the output of Algorithm 2 after privacy protection processing.

4.2 Privacy Protection Algorithm

As a secure design, this paper takes some measures to protect private information during the bidding process. The edge providers' cost is taken as an example for detailing privacy protection operations.

4.2.1 Sampling Edge Providers

There are many combinations of providers and their resource attributes. This paper chooses providers that respond to user requirements through sampling. Sampling is an approximate computing method. The reasons for sampling are threefold: (1) The sampling protects the information of providers who are not sampled. (2) Too many providers participating in the bidding would lead to high complexity and long computing time. The sampling of providers can help avoid this issue. (3) The sampling proportion of providers can be changed according to the demand. One important feature of simple random sampling (SRS) is that each sample has the same probability of being picked. SRS is fair, so this paper applies it to N edge providers to select E providers that will participate in the next process according to the sampling parameter s. This paper sets up a response group in

$EP_n, res_n = \langle p_n, Q_n, h_n \rangle$ *and* defines the SRS decision profile $\boldsymbol{x} = \{x_n\}, n \in N, x_n \in \{0, 1\}$. EP_n is chosen by the user if and only if $x_n = 1$. The information of these selected providers will be stored locally.

4.2.2 Differential Privacy

Edge providers selected though the SRS process adopts the differential privacy technology to protect their privacy. Normally, people do not want to answer sensitive questions. In cases where necessary information must be provided, vague items may be employed. Differential privacy is a method to protect information privacy by increasing noise. Considering the trade-off between data privacy and players' benefits, the parameter p can be calculated by uniform noise mechanism and discrete Laplacian mechanism [38]. The process of differential privacy works for one of the elements of res_n, such as p_n, which is as follows. First, generate a parameter $p \in (0, 1)$. Then, add the "noise". If the number is less than p, the provider responds with the true answer to the sensitive question, i.e., the price p_n. Otherwise, the provider offers a wrong answer which adds a noise value v_n to p_n. v is subject to Laplace distribution with scale parameter S_f/ε where S_f is the query sensitivity function:

$$p'_n = p_n + v_n \tag{16}$$

p'_n means the response price of EP_n. It is proved that the privacy mechanism has achieved ε-differential privacy [39]. Consider that a database produces transcript U on the set of queries $\boldsymbol{G} = \{G_1, \cdots, G_q\}$, and let $\varepsilon > 0$ be an arbitrarily small real constant. Transcript U satisfies ε-differential privacy that every pair of sibling datasets (D_1, D_2) meets $|D_1| = |D_2|$, while D_1 and D_2 differ in only one record, which holds that:

$$ln\frac{Pr[G^{D_1} = U]}{Pr[G^{D_2} = U]} \leq \varepsilon \tag{17}$$

The privacy budget ε specifies the amount of protection required, with smaller values corresponding to stricter protection. More importantly, after sampling and differential privacy processing, a higher degree of privacy protection can be achieved, named Zero-Knowledge privacy [40]. Meanwhile, as more data are collected, it can statistically eliminate the impact of probabilistic perturbations on overall. This privacy mechanism using probability s achieves ε_{ZK} privacy, which means that:

$$\varepsilon_{ZK} = ln(s \cdot \varepsilon\frac{2-s}{1-s} + 1 - s) \tag{18}$$

To protect the privacy of the user and edge providers, this paper designs Algorithm 2. Its input is $\{N, K_N, I_K^*, \omega_K, s, p, \lambda\}$, where N represents the set of all the providers, K_N is the set of all the providers' attributes, I_K suggests the importance of the attributes, s indicates the sampling proportion of the providers, p embodies the degree of differential privacy, and λ is the Laplace parameter. We can see that the complexity of Algorithms 1 and 2 are $O_{(\alpha E^2)}$ and $O_{(N)}$, respectively.

5 Experiments

In the simulation, this paper considers the scenario in which a user can jointly purchase resources from hundreds of edge providers deployed in various network infrastructures. The idle resources' types and numbers of the edge providers are limited. The benefit of the user to complete the tasks is fixed. The unit price of resources provided by each edge provider cannot exceed its cost. However, the unit cost of the same attribute resources may differ among edge providers. Each provider has idle resources, where the maximum value of idle resources owned by each provider varies from 0 to 100. Table 1 depicts the parameters of our secure edge resource bidding mechanism, and parts of them are referred to [41].

Algorithm 2: Privacy protection algorithm

```
Input: $N, K_N, I_K^*, \omega_K, s, p$, and $\lambda$
Output: $p'_E, Q'_E, h'_E$, and $Y$
normalize the attribute by Eq. (5);
calculate the QoS function $Q_N$ by Eq. (6);
initialize $p_N, h_N$ for all edge providers;
$\boldsymbol{Y} \leftarrow \varnothing, E = 0$;
for edge provider $n \in N$ do
    Random generation $R_{n1}, R_{n2} \in [0, 1]$;
    if $(R_{n1} < s)$ then
        $R'_{n2} = R_{n2}; p'_E = p_n; Q'_E = Q_n; h'_E = h_n; E = E + 1; \boldsymbol{Y} \leftarrow \boldsymbol{Y} \cup \{n\}$;
    end if
end for
for each $e \in \boldsymbol{Y}$ do
    if $(R'_{n2} \geq p)$ then
    $p'_e = p'_e + laplace(\lambda, 0)$;
    end if
end for
return $p'_E, Q'_E, h'_E, Y$
```

Table 1: System parameters

System parameters	Variable range	System parameters	Variable range
Number of edge providers	[500,2000]	Number of the resource attributes (K)	[5,100]
Cost of provider (h_n)	$\sum_{j\in K} \xi \cdot k_{n,j}^{\delta_2}/K$	The QoS value of the provider (Q_n)	$\sum_{j\in K} \gamma \cdot k_{n,j}^{\delta_1}/K$
User's revenue function (t)	$\sigma \cdot Z$	Differential privacy parameter (p)	[0,1]
Sampling parameter (s)	[0,1]	Normalizing process of attributes (M)	100
Laplace parameter (λ)	[0.01,1]	Quantity of resources required of user	[2000,2500]
Rewards of system (re)	[50,200]	Other parameter (G)	0.01

5.1 Effect of DMRBM

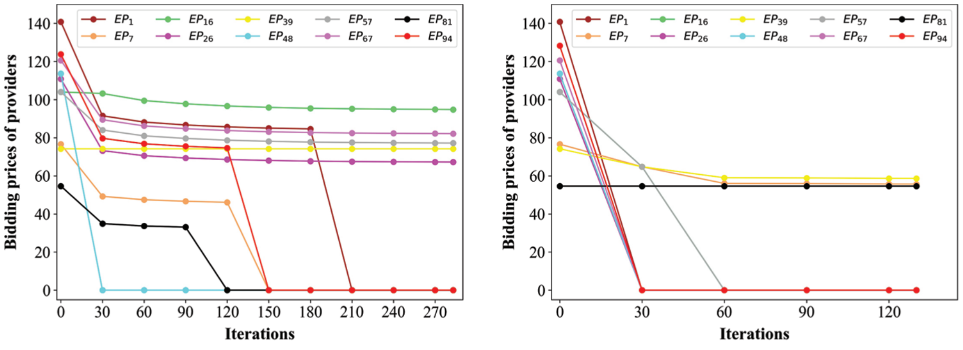
This paper evaluates the algorithm from three aspects: convergence, benefits of edge providers and the user, and the influence of privacy protection. Our experiment is based on the parameters in Table 2.

Table 2: Specific parameters in the experiment

Parameter	N	K	ξ	τ	γ	σ	δ_1	δ_2	$\bar{p}$
Value	1000	10	2	3	1.5	0.4	1	1.2	120

5.1.1 Convergence of DMRBM

The experiment is based on the 100 providers selected from 1000 providers through the privacy protection process. This paper describes how the prices of 10 edge providers change with the number of iterations and the results based on the PPR and LPR corresponding to Fig. 3 are not correlated.



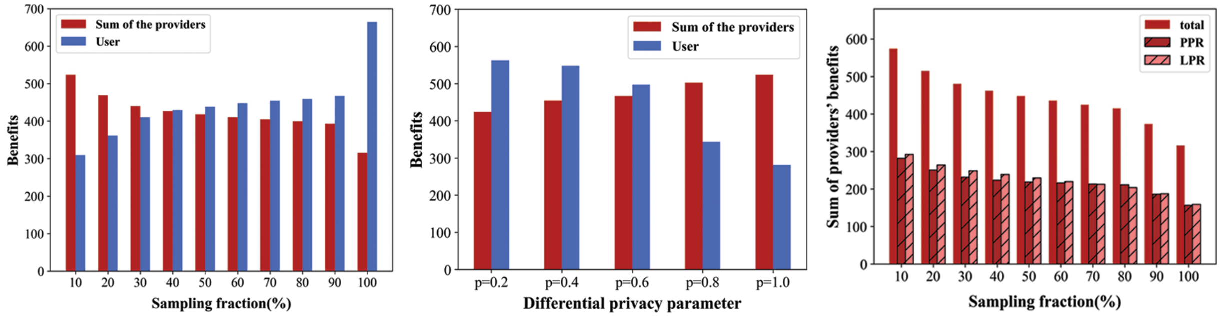
(a) (b)

Figure 3: (a) Prices with PPR and (b) prices with LPR

Fig. 3 shows the convergence process of bidding prices by the PPR and LPR evaluation functions in Algorithm 1. As the number of iterations increases, the bidding price decreases. Interestingly, these figures indicate that the providers' prices will reach a stable state, either 0 or the critical price p_e^*. Furthermore, some providers withdraw the bidding when the condition satisfies $p_e^* < h_e$ in PPR and $p_e^* < h_e - re_e$ in LPR. In Fig. 3b, we can find that the final prices of different providers are very close, but not exactly equivalent. This is due to the different rewards re_e of each edge provider. And the sublinear convergence of $\boldsymbol{p}_E^*$ and sequence $\boldsymbol{p}_E$.

5.1.2 Benefit Analysis between the User and N Edge Providers

The sums of the providers' and user's benefits are depicted in Fig. 4. It is most surprising that comparing the results of different sampling parameters (s = 0.9 and s = 1), there is a large increase in the user and a large decrease in the edge providers. There is a greater chance for the bidding based on all the providers to choose the better provider for the user than the bidding based on part providers.



(a) (b) (c)

Figure 4: (a) Benefits of providers and user by different sampling fractions, (b) benefits of providers and user by differential privacy parameter p with s = 10%, and (c) benefits of two evaluate functions

Fig. 4a analyzes the influence of the number of providers on the total benefits. We can see that as the number of edge providers increases, the gross benefits of the providers decline and the user's benefit increases. Fig. 4b illustrates that the differential privacy parameter p has a significant impact on the total benefits. The lower p means that the information used to compete deviates more from the initial information, and the larger p means that the information used to compete deviates less from the initial information. More surprisingly, when p is lower, the prices of the information after sampling will be closer to those before sampling. Fig. 4c demonstrates the sums of the providers and the benefits of the game based on the two evaluation functions separately. The user has the same preferences, which means i = j = 0.5. The benefits of the game based on LPR evaluation function are composed of two parts: the benefits of lower prices and the benefits of rewards. It is indicated that the benefits of only the pricing game are less than the benefits of a game based on PPR.

5.1.3 Performance Comparison of the Benefits

For fairly comparison, this paper uses two common resource pricing algorithms, CTOPD and PG-RL, respectively. The centralized task offloading and payment determination mechanism (CTOPD) is proposed by [42], which designs a centralized stable matching algorithm to make decisions on task offloading and the payment, but it only considers the stability of task offloading. The policy gradient (PG)-based reinforcement learning (RL) algorithm is proposed by [43], which enables continuous pricing, but it may overfit.

In the first simulation, this paper fixes the number of providers, N = 100. As shown in Fig. 5a, it is observed that the average benefits achieved by DMRBM are always higher than those achieved by the two comparison algorithms. Particularly, CTOPD only considers the match stability, it achieves the lowest benefits. In addition, PG-RL relies too much on historical information, which causes the average benefits to be lower than those of DMRBM. In the second simulation, this paper investigates the benefits that can be achieved by users and providers. Specifically, this paper fixes the number of users, while varying the number of providers from 20 to 100. As shown in Fig. 5b, this paper presents the system's user benefits. It is shown that with the increase in the number of providers, the average benefits of the users increase. This is reasonable. With more providers in the system, the users have more chances to buy the resources to gain higher benefits.

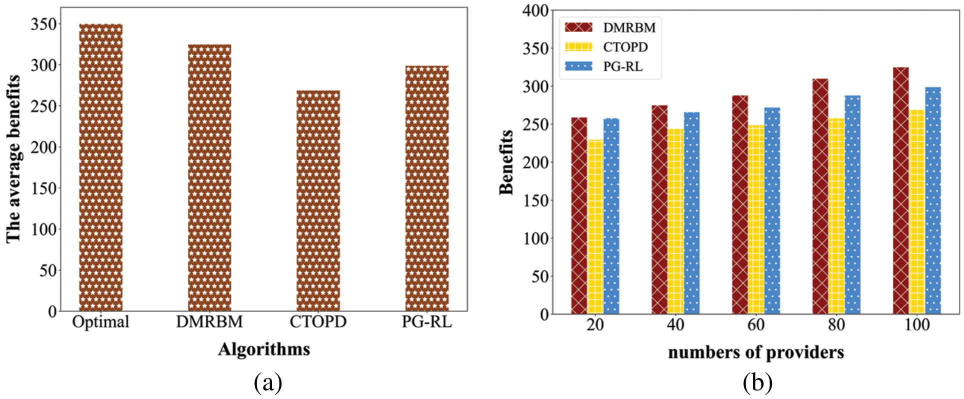
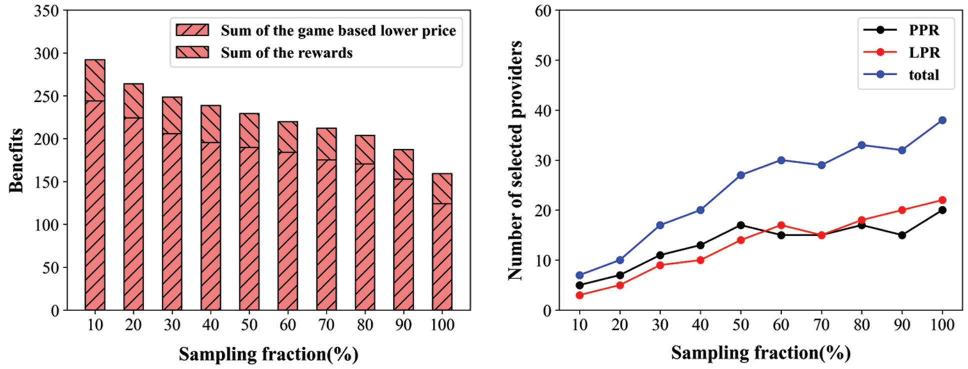


Figure 5: (a) The comparison on benefits and (b) benefits with numbers of providers

5.1.4 The Rewards of LPR

As mentioned above, we know that for the same QoS demands, the game based on PPR can get the highest benefits, so this paper needs to consider the benefits bought by a lower price and a reward respectively in the game based on LPR. As we can see from Fig. 6a, the benefits of a game based on lower prices outweigh those based on the rewards. Their benefits tend to be stable as the sample fractions increase. Although the total benefits decrease, the number of providers increases greatly, which corresponds to the expectations. As we can see from Fig. 6b, DMRBM increases the number of selected providers on the condition that the benefits of edge providers and users are maximized. The number of selected providers is greater than that of selected providers based on the PPR game or based on LPR game alone. Additionally, this paper finds that there are no inescapable links between the number of selected providers and the growth of sample fractions, nor do they inevitably increase one another.



(a) (b)

Figure 6: (a) Rewards of LPR with sampling fraction and (b) Number of optimal providers by PPR, LPR

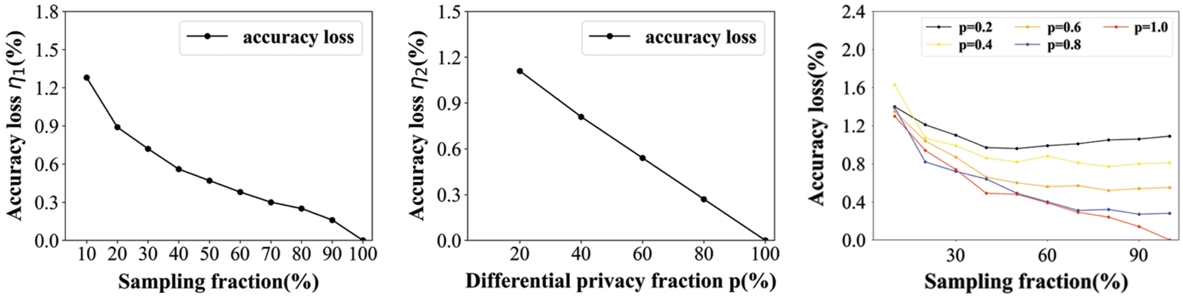
5.2 Effect of Privacy Protection Algorithm

This paper evaluates the effectiveness of the privacy protection process from two aspects: the accuracy loss of bidding caused by privacy protection and the degree of privacy protection.

5.2.1 Accuracy Loss of the Sampling and Differential Privacy

There could be a deviation since this paper estimates the total information based on the selected one. This paper calculates this deviation $\eta_1 = \frac{\sum_{n=1}^{N} p_n - x_n p_n \cdot \frac{N}{E}}{\sum_{i=1}^{E} p'_i}$. The accuracy loss η_2 represents the proportion of noise in the real value and is then defined as $\eta_2 = \frac{\sum_{i=1}^{E} \sqrt{(p'_i - p_i)^2}}{\sum_{i=1}^{E} p'_i}$. This paper estimates the impact of the sampling parameter s and differential privacy parameter p on the accuracy loss η_1 and η_2 respectively in Fig. 7. It depicts the total accuracy loss in the scenario of the ensured s and p in Fig. 7c. Because the total accuracy loss is caused by the sampling and differential privacy, this paper makes separate analyses in line with the losses caused by each step. In Fig. 7a, it first decreases noticeably as the sampling parameter s is gradually increased. This figure shows a steady decrease in the gradual increase of s. Fig. 7b also describes the trend that the more p increases, the less accuracy loss η_2

will present. In terms of total accuracy loss, we can see in Fig. 7c that as p increases, the total accuracy loss decreases first and then tends to be stable. The reason is that when the sampling parameter s is relatively small, the sampling accuracy loss is greater. When s is large, the factor that affects the accuracy loss is the operation of differential privacy. Only when the sampling fraction s approaches 1, p has a great impact on the accuracy loss. Fig. 7c is a lateral reflection of Figs. 7a and 7b.



(a) (b) (c)

Figure 7: (a) Accuracy loss $\boldsymbol{\eta}_1$ with sampling parameter s, (b) Accuracy loss $\boldsymbol{\eta}_2$ with the s, and (c) accuracy loss with sampling and differential privacy parameters

5.2.2 The Privacy Level of the Privacy Protection

This paper measures the degree of privacy protection ε_{ZK} after performing sampling and differential privacy. The privacy is measured by the level of achieved zero-knowledge privacy by Eq. (18). In this case, this paper uses the same sampling parameter s = 0.5 to calculate the privacy level of the differential privacy parameter p. Table 3 shows how different p parameter settings affect privacy. The smaller ε_{ZK} is, the higher the degree of privacy protection will be. This result also fits into the definition of privacy level, which decreases as the probability of truthful answers increases.

Table 3: Privacy level with differential privacy parameter p

p	Privacy level (ε_{ZK})
0.2	1.421386
0.4	1.504077
0.6	1.749200
0.8	1.951292
1.0	2.152393

6 Conclusion

Our study focuses on edge providers' resource bidding and privacy security issues in the bidding process. Our aims are to protect the privacy of the edge providers and users and to find reasonable prices in the resource bidding for more diverse edge providers. This paper proposes a secure edge resource bidding mechanism based on approximate computing, differential privacy, and game theory. The combination of these methods makes the competition result of sampled data and differential privacy information become as close as possible to the competition result of real information. At the same time, it can not only protect the edge providers' private information but also choose the proper providers and reasonable prices through the providers' two evaluation functions (namely PPR and LPR) in the DMRBM. The feasibility of this mechanism is verified by a large number of simulation results and comparisons with the existing technologies and benchmark schemes.

Funding Statement: This work was supported in part by National Natural Science Foundation of China under Grant No. 62172349, 62032020, and 62172350, the Research Foundation of Education Bureau of Hunan Province under Grant No. 21B0139, the National Key Research and Development Program of China under Grant 2021YFB3101200, Hunan Science and Technology Planning Project under Grant No. 2019RS3019.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] L. He, K. Ota and M. Dong, "Learning IoT in edge: Deep learning for the internet of things with edge computing," *IEEE Network*, vol. 32, no. 1, pp. 96–101, 2018.

[2] Y. Mao, C. You, J. Zhang, K. Huang and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.

[3] J. Wang, L. Zhao, J. Liu and N. Kato, "Smart resource allocation for mobile edge computing: A deep reinforcement learning approach," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 3, pp. 1529–1541, 2021.

[4] F. Li, H. Yao, J. Du, C. Jiang, Z. Han *et al.,* "Auction design for edge computation offloading in SDN-based ultra dense networks," *IEEE Transactions on Mobile Computing*, vol. 21, no. 5, pp. 1580–1595, 2020.

[5] T. Liu, S. Ni, X. Li, Y. Zhu, L. Kong *et al.,* "Deep reinforcement learning based approach for online service placement and computation resource allocation in edge computing," *IEEE Transactions on Mobile Computing*, 2022. https://doi.org/10.1109/TMC.2022.3148254.

[6] Y. Nakamura, T. Mizumoto, H. Suwa, Y. Arakawa, H. Yamaguchi *et al.,* "In-situ resource provisioning with adaptive scale-out for regional IoT services," in *2018 IEEE/ACM Symp. on Edge Computing (SEC)*, Seattle, USA, pp. 203–213, 2018.

[7] Z. Junhui, Y. Tao, G. Yi, W. Jiao and F. Lei, "Power control algorithm of cognitive radio based on non-cooperative game theory," *China Communications*, vol. 10, no. 11, pp. 143–154, 2013.

[8] W. Lu, S. Zhang, J. Xu, D. Yang and L. Xu, "Truthful multi-resource transaction mechanism for P2P task offloading based on edge computing," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 6122–6135, 2021.

[9] K. Xiao, W. Shi, Z. Gao, C. Yao and X. Qiu, "DAER: A resource preallocation algorithm of edge computing server by using blockchain in intelligent driving," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9291–9302, 2020.

[10] T. Liu, H. Guo, C. Danilov and K. Nahrstedt, "A privacy-preserving data collection and processing framework for third-party UAV services," in *2020 IEEE 19th Int. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Guangzhou, China, pp. 683–690, 2020.

[11] C. Piao, Y. Shi, J. Yan, C. Zhang and L. Liu, "Privacy-preserving governmental data publishing: A fog-computing-based differential privacy approach," *Future Generations Computer Systems: FGCS*, vol. 90, no. 1, pp. 158–174, 2019.

[12] L. Hartmann, "Bounded privacy: Formalising the trade-off between privacy and quality of service," in *Lecture Notes in Informatics (LNI)*, Bonn: Gesellschaft für Informatik, pp. 267–272, 2018.

[13] J. Zhang, S. Pourazarm, C. G. Cassandras and I. C. Paschalidis, "The price of anarchy in transportation networks: Data-driven evaluation and reduction strategies," *Proceedings of the IEEE*, vol. 106, no. 4, pp. 538–553, 2018.

[14] W. Huang, S. Zhou, T. Zhu and Y. Liao, "Privately publishing internet of things data: Bring personalized sampling into differentially private mechanisms," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 80–91, 2022.

[15] B. Baek, J. Lee, Y. Peng and S. Park, "Three dynamic pricing schemes for resource allocation of edge computing for IoT environment," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4292–4303, 2020.

[16] 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.

[17] R. Berardo and M. Lubell, "The ecology of games as a theory of polycentricity: Recent advances and future challenges," *Policy Studies Journal*, vol. 47, no. 1, pp. 6–26, 2019.

[18] G. Benita Nancy and J. J. V. Nayahi, "Bidirectional bidding for efficient allocation of multiple resources in clouds," in *2016 Int. Conf. on Recent Trends in Information Technology (ICRTIT)*, Chennai, India, pp. 1–8, 2016.

[19] K. Xie, X. Wang, G. Xie, D. Xie, J. Cao *et al.,* "Distributed multi-dimensional pricing for efficient application offloading in mobile cloud computing," *IEEE Transactions on Services Computing*, vol. 12, no. 6, pp. 925–940, 2019.

[20] H. Zhang, Y. Xiao, S. Bu, D. Niyato, F. R. Yu *et al.,* "Computing resource allocation in three-tier IoT fog networks: A joint optimization approach combining stackelberg game and matching," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1204–1215, 2017.

[21] M. Yu, A. Liu, N. N. Xiong and T. Wang, "An intelligent game-based offloading scheme for maximizing benefits of IoT-edge-cloud ecosystems," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 5600–5616, 2022.

[22] R. Begam, W. Wang and D. Zhu, "TIMER-Cloud: Time-sensitive VM provisioning in resource-constrained clouds," *IEEE Transactions on Cloud Computing*, vol. 8, no. 1, pp. 297–311, 2020.

[23] J. Guo, G. Huang, Q. Li, N. N. Xiong and S. Zhang, "STMTO: A smart and trust multi-UAV task offloading system," *Information Sciences*, vol. 573, no. 1, pp. 519–540, 2021.

[24] X. Z. You and S. Zhang, "A kind of network security behavior model based on game theory," in *Int. Conf. on Parallel & Distributed Computing*, Chengdu, China, pp. 950–954, 2003.

[25] C. P. Ram and G. Sreenivaasan, "Security as a Service (SasS): Securing user data by coprocessor and distributing the data," in *Trendz in Information Sciences & Computing (TISC2010)*, Chennai, India, pp. 152–155, 2010.

[26] B. Gu, L. Gao, X. Wang, Y. Qu, J. Jin *et al.,* "Privacy on the edge: Customizable privacy-preserving context sharing in hierarchical edge computing," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 2298–2309, 2020.

[27] M. Ramasamy, G. Narmadha and S. Deivasigamani, "Carry based approximate full adder for low power approximate computing," in *7th Int. Conf. on Smart Computing & Communications (ICSCC)*, Harbin, China, pp. 1–4, 2019.

[28] P. Zeng, A. Liu, C. Zhu, T. Wang and S. Zhang, "Trust-based multi-agent imitation learning for green edge computing in smart cities," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 3, pp. 1635–1648, 2022.

[29] W. Yang and H. Thapliyal, "Approximate adiabatic logic for low-power and secure edge computing," *IEEE Consumer Electronics Magazine*, vol. 11, no. 1, pp. 88–94, 2022.

[30] L. Lei, H. Xu, X. Xiong, K. Zheng and W. Xiang, "Joint computation offloading and multiuser scheduling using approximate dynamic programming in NB-IoT edge computing system," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5345–5362, 2019.

[31] P. Derbeko, S. Dolev, E. Gudes and J. D. Ullman, "Efficient and privacy preserving approximation of distributed statistical queries," *IEEE Transactions on Big Data*, vol. 8, no. 5, pp. 1399–1413, 2022.

[32] Y. Wang, X. Lou, Z. Fan, S. Wang and G. Huang, "Verifiable multi-dimensional (t,n) threshold quantum secret sharing based on quantum walk," *International Journal of Theoretical Physics*, vol. 61, no. 2, pp. 1–17, 2022.

[33] M. Dabbagh, K. K. R. Choo, A. Beheshti, M. Tahir and N. S. Safa, "A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities," *Computers & Security*, vol. 100, no. 1, pp. 102078, 2021.

[34] Y. Huo, C. Meng, R. Li and T. Jing, "An overview of privacy preserving schemes for industrial internet of things," *China Communications*, vol. 17, no. 10, pp. 1–18, 2020.

[35] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu *et al.,* "Edge computing in VANETs-An efficient and privacy-preserving cooperative downloading scheme," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1191–1204, 2020.

[36] L. Gao, S. Deng and W. Ren, "Differentially private consensus with an event-triggered mechanism," *IEEE Transactions on Control of Network Systems*, vol. 6, no. 1, pp. 60–71, 2019.

[37] G. V. Prasad, A. S. Prasad and S. Rao, "A combinatorial auction mechanism for multiple resource procurement in cloud computing," *IEEE Transactions on Cloud Computing*, vol. 6, no. 4, pp. 904–914, 2018.

[38] Q. Geng and P. Viswanath, "Optimal noise adding mechanisms for approximate differential privacy," *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 952–969, 2016.

[39] F. Mcsherry, K. Nissim and A. Smith, "Calibrating noise to sensitivity in private data analysis," *Lecture Notes in Computer Science*, vol. 3876, no. 8, pp. 265–284, 2012.

[40] J. L. Rrushi, "DNIC architectural developments for 0-Knowledge detection of OPC malware," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 1, pp. 30–44, 2021.

[41] J. Hu, K. Li, C. Liu and K. Li, "A game-based price bidding algorithm for multi-attribute cloud resource Provision," *IEEE Transactions on Services Computing*, vol. 14, no. 4, pp. 1111–1122, 2021.

[42] X. Wang, J. Wang, X. Zhang, X. Chen and P. Zhou, "Joint task offloading and payment determination for mobile edge computing: A stable matching based approach," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12148–12161, 2020.

[43] S. Chen, L. Li, Z. Chen and S. Li, "Dynamic pricing for smart mobile edge computing: A reinforcement learning approach," *IEEE Wireless Communications Letters*, vol. 10, no. 4, pp. 700–704, 2021.