sensors

Article

# SecMDGM: Federated Learning Security Mechanism Based on Multi−Dimensional Auctions

Qian Chen [1,2,3], Lin Yao [4], Xuan Wang [1,2,3,*], Zoe Lin Jiang [1,2,3], Yulin Wu [1,3] and Tianzi Ma [1,3]

[1] School of Computer Science and Technology, Harbin Institute of Technology Shenzhen, Shenzhen 518000, China
[2] Peng Cheng Laboratory, Shenzhen 518000, China
[3] Guangdong Provincial Key Laboratory of Novel Security Intelligence Technologies, Shenzhen 518000, China
[4] School of Software, Harbin Institute of Technology, Harbin 150000, China
[*] Correspondence: wangxuan@cs.hitsz.edu.cn

**Abstract:** As a newly emerging distributed machine learning technology, federated learning has unique advantages in the era of big data. We explore how to motivate participants to experience auctions more actively and safely. It is also essential to ensure that the final participant who wins the right to participate can guarantee relatively high−quality data or computational performance. Therefore, a secure, necessary and effective mechanism is needed through strict theoretical proof and experimental verification. The traditional auction theory is mainly oriented to price, not giving quality issues as much consideration. Hence, it is challenging to discover the optimal mechanism and solve the privacy problem when considering multi−dimensional auctions. Therefore, we (1) propose a multi−dimensional information security mechanism, (2) propose an optimal mechanism that satisfies the Pareto optimality and incentive compatibility named the SecMDGM and (3) verify that for the aggregation model based on vertical data, this mechanism can improve the performance by 2.73 times compared to that of random selection. These are all important, and they complement each other instead of being independent or in tandem. Due to security issues, it can be ensured that the optimal multi−dimensional auction has practical significance and can be used in verification experiments.

**Keywords:** game theory; federated learning; mechanism design; auction theory; partial homomorphic encryption

**Citation:** Chen, Q.; Yao, L.; Wang, X.; Lin Jiang, Z.; Wu, Y.; Ma, T. SecMDGM: Federated Learning Security Mechanism Based on Multi−Dimensional Auctions. *Sensors* **2022**, *22*, 9434. https://doi.org/10.3390/s22239434

Academic Editors: Thippa Reddy Gadekallu, Kuruva Lakshmanna and Rutvij Jhaveri

Received: 12 October 2022
Accepted: 30 November 2022
Published: 2 December 2022

## 1. Introduction

With the deep integration and application of artificial intelligence in different industries [1–3] and social life [4–6], model training needs more participants. In this paper, we discuss how to motivate participants to provide their multi−dimensional information, such as data [7,8] and computing power.

However, data privacy and security risks [9,10] have caused widespread concern and even anxiety and panic. Federated learning [11–14] is attracting increasing attention as it can build aggregation models by ensuring that there is no need to submit raw data outside the local area [15–17]. Federated learning plays a perfect role in protecting privacy in model aggregation [18,19], but a suitable mechanism is needed to motivate someone to participate in this task before computing. Zhan et al. [20,21] focused on how to motivate clients effectively to participate in federated learning reliably and conducted extensive research on the existing work about incentive mechanisms for federated learning. From an economic perspective, federated learning only provides a technology but does not consider why the clients should participate or what benefits they can gain. However, Zhan et al. did not consider security and multi−dimensional information in the mechanism. Therefore, we need to provide a better mechanism for federated learning.

We need a standard and unified framework and theory with which we can compare and research the advantages and disadvantages of mechanisms [22,23] in the resource allocation and system design of federated learning. This is why we thought of the theory of auction mechanism design [24–26]. A suitable mechanism allows the game decision to obtain better payoffs, ceteris paribus, and it is applied in many fields [6,27,28]. In the latest edition of Nature, DeepMind [7] discusses human−centered mechanism design options. The design of the mechanism is present in almost all resource allocation issues, including taxation, voting, and spectrum auctions.

The three critical mechanism design theories are auction, contract, and bargaining. In the 1960s, William Vickrey [29] and Armando Ortega Reichert made pioneering contributions to auction theory. The 2020 Nobel Prize in economics was awarded to Paul Milgrom for his contributions to improving auction theory and new auction forms. As he said, when a traditional economic theory cannot explain and calculate the complex scenes of reality, we require a high−performance computing solution based on traditional theory to evaluate the mechanisms, getting better social welfare in the meanwhile. Therefore, it is ideal to explore the challenges of federated learning by mechanism design.

The most well−known application of auction theory, on which this paper is based, includes advertising positions [30,31] and antique auctions. However, all problems related to resource allocation are inseparable from auction theory. This is a completely theoretical system that goes far beyond the auction application. First−price auction is a simple process [32] in which many buyers bid on an item and the highest bidder procures the item (paying the highest bidding price).

Homomorphic encryption is a unique method supporting algebraic operations in ciphertext data. It plays a central role in the security mechanism discussed in this paper. On the Internet, clients in federated learning need to not only compete for participation but also ensure the quality and security of the winner. Therefore, it is necessary to develop an improved auction mechanism. It is critical to ensure that the bidding information is not intercepted by competitors or leaked and that the clients submit real multi−dimensional information. Hence, a secure multi−dimensional optimal auction mechanism is crucial.

The ubiquitous online advertising [33,34] auction faces a similar security problem as federated learning. This is just a snapshot of many scenes we have not explored yet, and the mechanical design of federated learning discussed in this paper is one of the most representative. As it considers not only the security during the auction but also the quality after the auction, it requires studying a multi−dimensional mechanism. Traditional auctions are price−oriented, and considering only price will lead to sacrificing quality. However, when participants are requested to provide information other than price, such as multi−dimensional information about their counting ability, this can compromise their privacy. This seems to be a contradiction. Therefore, we need to explore a secure auction mechanism for federated learning that can guarantee the quality of participants and the privacy of multi−dimensional information. We solve this problem for the first time by designing security mechanisms named the SecMDGM for multi−dimensional information in federated learning.

The optimal mechanism is for participants to voluntarily provide information regarding their actual price and computing power and other multi−dimensional information. An auction with this feature is called "strategy−proof," and the auction mechanism that follows this winner−pick rule is called the "direct mechanism." The idea of strategy−proof as the core of auction design was first given by the American Nobel Prize winner William Vickery. However, does this still hold for the case of multi−dimensional encrypted messages? Designing a mechanism to maximize the expected profit and satisfy the Pareto equilibrium and incentive compatibility is necessary, which is addressed in Section 3.

Figure 1 provides the framework of the SecMDGM mechanism, including the auction stage (select the participant) and the calculation stage (agglomerate the model) of federation learning. Unlike other research on federated learning, we consider both quality and security for the first time. This is why we do not compare it with other papers in an experiment in Section 4. Briefly, we focus more on the right side in Figure 1. This paper is an extension of federated learning.

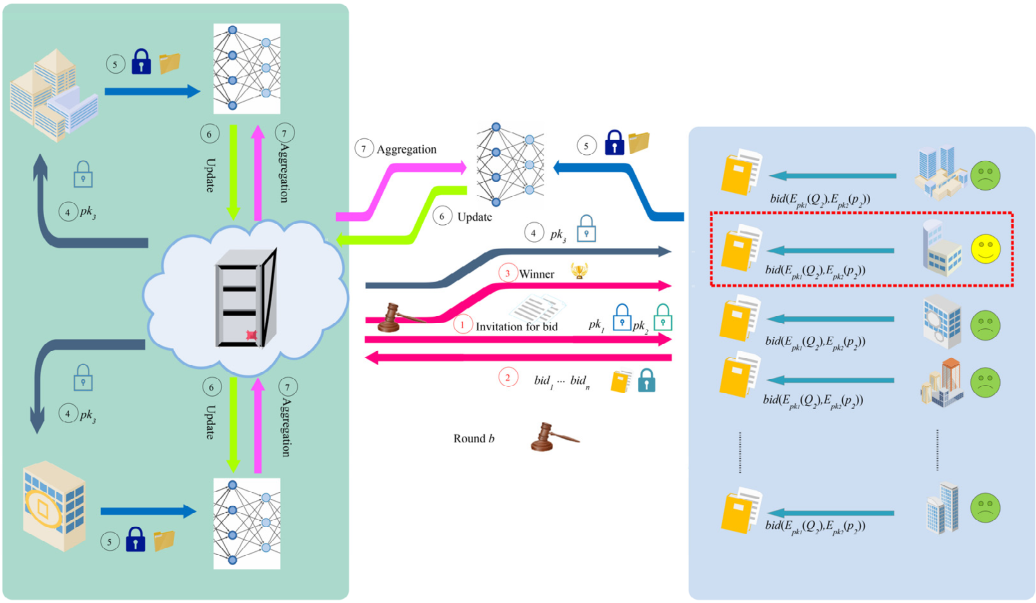

5
6 Update
7 Aggregation
4 $pk_3$
7 Aggregation
6 Update
5
4 $pk_3$
3 Winner
1 Invitation for bid
$pk_1$ $pk_2$
2 $bid_1 \cdots bid_n$
Round $b$
$bid(E_{pk1}(Q_2),E_{pk2}(p_2))$
$bid(E_{pk1}(Q_2),E_{pk2}(p_2))$
$bid(E_{pk1}(Q_2),E_{pk2}(p_2))$
$bid(E_{pk1}(Q_2),E_{pk2}(p_2))$
$bid(E_{pk1}(Q_2),E_{pk2}(p_2))$

**Figure 1.** Framework for the design of federated learning security mechanisms.

This paper explores how to make different participants more active in federated learning upfront and ensure that the final winner can provide a higher−quality model instead of a low price. Meanwhile, focuses on the privacy protection of personal multi−dimensional data. To sum up, the contributions of this paper are as follows:

(1) Security:
    (1) We realized the computation of the ciphertext score function for mechanism design based on partial homomorphic.
    (2) We redeployed the federated learning process to cover bid submission, auction calculation, and model aggregation security.

(2) Necessity:
    (1) The mechanism proposed in this paper considers the multi−dimensional information of bidders, which is more in line with actual demand.
    (2) It is proved that our mechanism is Pareto optimal and satisfies incentive compatibility (IC), which is the primary measure of mechanism performance.
    (3) It is proved that the mechanism can maximize the participants' profit, and the equation and proof of the optimal strategy are provided.

(3) Effectiveness:
    (1) Experiments show that our mechanism can improve the accuracy of the federated learning model while ensuring security.
    (2) Our mechanism is also suitable for vertical data.

The rest of this paper is organized as follows: Section 2 presents the work on mechanism design, federated learning, and cryptographic algorithms and the relationship between them. Section 3 theoretically proves the security and necessity of the proposed multi−dimensional security mechanism. In Section 4, the effectiveness of the proposed mechanism is experimentally verified. Section 5 provides the conclusion.

## 2. Preliminaries and Notations

This paper explores the secure federated learning mechanism under multi−dimensional information for the first time from the game theory perspective. Not only does it guarantee the feasibility of security in multi−dimensional auctions, it also proves that the multi−dimensional mechanism can obtain a dominant strategy in the cryptographic process and satisfies incentive compatibility, which also enables participants to obtain the maximum expected revenue.

Since many fields of knowledge are involved here, Section 2.1 introduces auction theory in mechanism design and the difficulty of multi−attribute auctions, Section 2.2 discusses partial homomorphic encryption and its security guarantees, and Section 2.3 discusses the vertical federation learning model.

They are interdependent, and multi−dimensional auctions can only provide the optimal mechanisms in theory. They cannot guarantee the feasibility of the application because participants will be reluctant to submit crucial information for fear of their privacy being compromised, even if they know that this is the optimal strategy. Partial homomorphic encryption solves this problem. As a new distributed solution, computing security in federated learning has also been deeply explored. However, in addition to the security of the calculation itself, security is necessary for the participant selection stage as well, especially when the participants are providing multi−dimensional private information instead of simply price. High−quality participants decide the performance of the final aggregation model.

### *2.1. Multi−Dimensional Auction and Mechanism Design*

In this paper, the design of the federated learning mechanism is the core issue. Even the discussion about security and quality is based on the mechanism design itself. Therefore, the most crucial thing is comprehending the mechanism design theory and the relationship between mechanism design and auction theory in federated learning.

The principal−agent model is the basic analytical framework of mechanism design theory, as shown in Figure 2. First, the principal designs a mechanism, which is the main contribution of this paper. Second, multiple participants compete to participate in federated learning according to the given auction mechanism. Auction, bargaining, and cooperation theory are the three major mechanism design theories. An auction is a market mechanism in which participants make bids and determine the allocation of resources and the price paid according to a set of defined rules [35]. Paul Milgrom was awarded the Nobel Prize in Economics for his important contributions to auction theory.

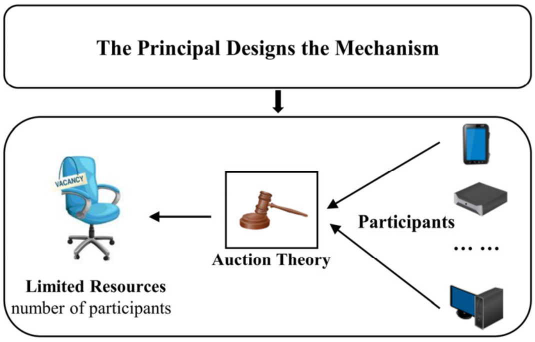


**Figure 2.** The relationship between mechanism design and auction theory in federated learning.

We abstract the limited participating resources on the server as the auction object of the mechanism, and the participants who want to participate in the model aggregation become buyers. Under the optimal mechanism, the service provider can maximize social welfare by selecting the best participant, which can be the best performance of the focusing function. Each participant can honestly provide the highest−quality bidding information for maximum benefit. Under the optimal mechanism, the service provider can improve the performance of the aggregation function by selecting the right participants to maximize social welfare.

Mechanism design theory provides ways to avoid these dilemmas under specific circumstances. Dominant mechanisms allow participants to show their personal preferences and achieve social goals. To better understand the auction mechanism, we list examples of a first−price auction. As shown in Figure 3, in the first−price auction, each participant uses a specific value to bid for the item [36,37]. At this time, the auction mechanism must make two decisions. First, who will obtain the item? It can be seen that the third participant obtained the item, with the highest bid price. Second, what amount needs to be paid? The winner needs to pay USD 8. This is one of the most manageable single−dimensional auctions that can help us understand the multi−dimensional auction theory better.

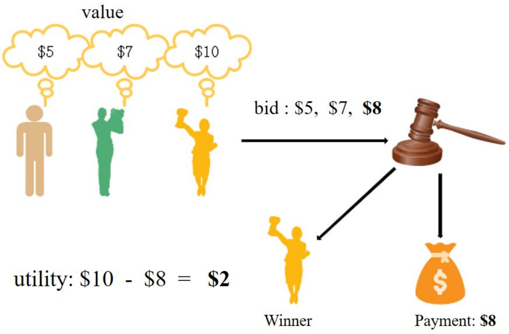


**Figure 3.** First−price auction of a single dimension.

In the traditional mechanism design, the VCG auction mechanism satisfies the conditions of incentive compatibility (IC) and individual rationality (IR), which can maximize the expected profit of participants. This is effective in single−item single−dimensional auctions, but single−item multi−attribute auctions require further exploration.

**Definition 1.** *VCG Mechanism.*

The allocation $x(b)$ and payment rules $p(b)$ of the VCG mechanism satisfy the following two equations, respectively:

$$x_i(b) = \underset{\omega\in\Omega}{argmax} \sum_{i=1}^{n} b_i(\omega) \tag{1}$$

$$p_i(b) = (\underset{\omega\in\Omega}{max} \sum_{j\neq i} b_j(\omega)) - \sum_{j\neq i} b_j(\omega^*) \tag{2}$$

where $b$ stands for the bid of the participants

Here, is an alternative formula representation of the payment rules in the VCG mechanism.

$$p_i(b) = b_i(\omega^*) - [\sum_{j=1}^{n} b_j(\omega^*) - \underset{\omega\in\Omega}{max} \sum_{j\neq i} b_j(\omega)] \tag{3}$$

This can help us better understand the theoretical proof of the SecMDGM mechanism in Section 3. The multi−dimensional auction originated from the requirements of the U.S. Department of Defense for the procurement and supply of weapons. Competitive procurement of weapons considers not only price but also various performance metrics of the weapon, including technical characteristics, delivery dates, labor performance, and estimated program costs. Equation (4) provides a simple score function for measuring the mechanism design, which is related to the utility function and price $p$ induced by the multi−dimensional feature information $Q = (q_1, q_2, \cdots, q_m)$.

$$Score = U(q_1, \cdots, q_m) - p \tag{4}$$

Bichler defined multi−dimensional auction [38] as an auction mode in which multiple attributes of the item are considered when buyers and sellers trade, that is, an auction mode in which the two parties conduct multiple negotiations on other quality attributes in addition to the price. The experimental research shows that, for buyers, the multi−dimensional auction is better than the single−dimensional auction. Sometimes, the situation of suppliers will also improve. However, we improve the multi−dimensional auction theory via practical applications in federated learning and avoid the leakage of private information by guaranteeing security.

Many practical and theoretical problems, such as the formulation of laws and regulations, administrative management, and democratic elections, can be transformed into mechanism design problems. This paper translates the federated learning problem into an optimization problem for the auction mechanism, and the proof and measurement index of the SecMDGM mechanism is provided in Section 3.

### *2.2. Partial Homomorphic Encryption*

Compared with the single−dimensional auction, the multi−dimensional auction can improve the quality of the participants but requires providing more personal information. From a theoretical point of view, multi−attribute auctions are enough. However, from a practical point of view, we need to design a multi−attribute auction mechanism and ensure the security of the bidding information. Therefore, the SecMDGM mechanism needs the support of cryptography.

Homomorphic encryption [39] can support algebraic operations of ciphertext. To satisfy the requirements of confidentiality, cryptographers have designed different types of encryption methods according to different NP−hard problems. According to the different computing powers, these can be divided into partial and fully homomorphic encryption. Unlike the slower computation of fully homomorphic encryption [33–35], partial homomorphic encryption [40] is compatible with our auction mechanism in terms of security and computation performance. This is the first time that the security method and the multi−dimensional mechanism have been skillfully combined and provide strict theoretical proof.

The Paillier encryption algorithm is a representative additive homomorphic algorithm invented by Paillier in 1999 [41], based on the difficult question in the compound residual category. Moreover, the RSA encryption algorithm is the first that can be used for encryption and digital signatures that are easy to understand and operate. After surviving various attacks, it has gradually become widely accepted. It is generally considered one of the best public key cryptography algorithms and representative of multiplicative homomorphism algorithms. The SecMDGM mechanism skillfully uses the characteristics of Paillier and RSA encryption algorithms and applies them to the auction mechanism.

In this paper, fully homomorphic encryption is not considered because (1) it will be costly in terms of time and (2) the server is completely trustworthy in federated learning. Security can be achieved by adding several encryption and decryption calculations. Therefore, because the time cost of a partially homomorphic encryption algorithm can be completely ignored, this paper does not make an experimental comparison of time complexity.

In this paper, partial homomorphic encryption provides theoretical support for security calculation. A public−key cryptosystem, for all keys ($pk$, $sk$), that is generated by the key generation algorithm $Gen(1^n)$, has a plaintext space $M$ and a ciphertext space $C$. For messages $m_1, m_2 \in M$ in plaintext space, the corresponding ciphertext data $c_1 = E_{pk}(m_1)$ and $c_2 = E_{pk}(m_2)$ satisfy Equation (5).

$$Dec_{sk}(c_1 \circ \mathrm{c}_2) = m_1 \circ m_2 \tag{5}$$

If the operator $\circ$ is an additive operation, homomorphic encryption is called additive homomorphic. If it is a multiplicative operation, it is called multiplicative homomorphic. If an encryption method is homomorphic to only one operation, it is called partial homomorphic encryption. Otherwise, it is called fully homomorphic encryption. We prove the security of the encryption algorithms of Paillier and RSA as follows.

#### 2.2.1. The Security of Paillier Additive Homomorphic Encryption

The encryption and decryption process of Paillier, where $pk_2$ = ($n$, $g$) is the public key and $sk_2$ = ($\lambda$, $\mu$) is the private key, is as follows:

First, the key needs to be generated.

(1) Randomly choose two large prime numbers $p$ and $q$ that satisfy $gcd(pq, (q-1)) = 1$ and satisfy $p$ and $q$ of equal length.
(2) Calculate $n = pq$ as well as $\lambda = lcm(p-1, q-1)$. Here, $lcm$ denotes the least common multiple.
(3) Randomly select integer $g \in Z_{n^2}^*$.
(4) Define the function $L(x) = \frac{x-1}{n}$ and calculate $\mu = \left(L\left(g^{\lambda} modn^2\right)\right)^{-1} modn$.

Here, is Paillier's encryption process.

(1) Input a plaintext $m$ that satisfies $0 \leq m \leq n$.
(2) Choose a random number $r$ that satisfies $0 \leq r < n$ and $r \in Z_n^*$.
(3) Calculate the ciphertext $c = g^m r^n mod\ n^2$.

Paillier's decryption process is as follows:

(1) Input a ciphertext message $c$ that satisfies $c \in Z_{n^2}^*$.
(2) Calculate the plaintext $m = L\left(c^{\lambda} mod\ n^2\right) * \mu modn$.

Paillier satisfies the standard definition of security for encryption schemes, semantic security, i.e., indistinguishability under chosen−plaintext attack (IND−CPA). Intuitively, the ciphertext does not reveal any information in plaintext. The security of Paillier can be reduced to the decisional composite residuosity assumption (DCRA), i.e., given a composite number $n$ and an integer $z$. It is NP−hard to determine whether $z$ is $n$ times residual under mod $n^2$, i.e., whether there exists $y$ satisfying $z \equiv y^n \left(mod\ n^2\right)$.

### 2.2.2. The Security of RSA Multiplicative Homomorphic Encryption

Assuming that the ciphertext is c and the plaintext is m, the encryption process of RSA is as follows:

$$c = m^E \mathrm{mod} N \tag{6}$$

where $pk_1 = (E, N)$ is the public key and $sk_1 = (D, N)$ is the private key. Here, we use the public key to encrypt and the private key to decrypt. When $N = p*q$, $L = lcm(p-1, q-2)$, and $gcd(E, L) = 1$ are satisfied when $1 < E < L$ and $E*D$ mod $L = 1$ when $1 < D <$ L, the key is generated.

The decryption process of RSA is as follows:

$$m = c^D \mathrm{mod} N \tag{7}$$

The security of the RSA encryption scheme depends on whether the attacker can quickly obtain the plaintext $m$. The easy method is to obtain the plaintext $m$ by finding the private key $D$. To obtain the private key $D$, we need to decompose $N$ into $p$ and $q$ and then calculate $p-1$ and $q-1$ to derive $D$ from $E$. Thus, the security of RSA relies on the knowledge of number theory that factorizing a large integer's prime factor is difficult and inefficient. Briefly, it relies on the difficulty of factoring large numbers. There is no polynomial−time method for factoring the decomposition of large factors.

Figure 1 shows the overall framework of this article. The secure computing of federated learning refers to steps 4 to 7 with $pk_3$, which experts have thoroughly studied. Our research focuses on steps 1 to 3, with $pk_1$ and $pk_2$ corresponding to RSA and Paillier, which are not in traditional federated learning. With these steps, clients can participate more actively in model aggregation. The improvement of the multi−dimensional auction has further improved the quality of the winner. In addition, the guarantee of partial homomorphic encryption ensures that participants are no longer worried about data leakage. In Section 3, we directly use *Encrypt*/*E*() and *Decrypt*/*D*() to represent the encryption and decryption functions.

## *2.3. Vertical Federated Learning*

The Google team [42] initially proposed federated learning to explore a predictive model that enables multiple smartphones to learn and share cooperatively. Different from traditional distributed learning, it can aggregate models without taking the original parameters out of the local area. The key Equation (8) is as follows:

$$\omega(t+1) = \frac{\sum_{i=1}^{N} C_i \omega_i(t+1)}{\sum_{i=1}^{N} C_i} \tag{8}$$

where $C_i$ is the weight of the participants

One of the important issues unsolved in federated learning is the non−independent homogeneous distribution of data. The SecMDGM mechanism of this paper involves this problem because it measures multi−dimensional information and more dimensional information can provide a higher−quality winner for the server.

Traditional horizontal federated learning considers that two datasets have more overlapping features and fewer overlapping users. However, in real situations, the data providers in horizontal federated learning often compete.

As shown in Figure 4, each column represents the respective features of the participants. Since the features of the participants are different, it does not satisfy an independent homogeneous distribution. However, vertical federated learning that considers multi−dimensional data can improve the model's accuracy.

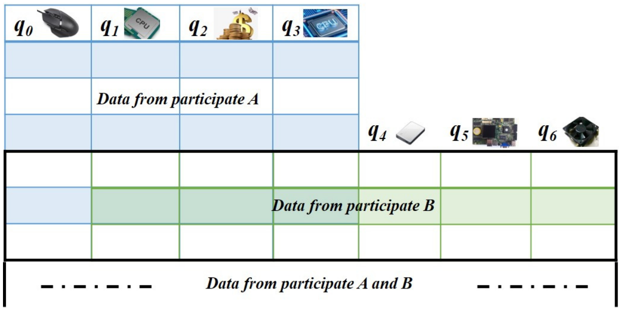


**Figure 4.** Vertical federated learning of multi−dimensional data.

Therefore, we design an incentive mechanism based on vertical data. Vertical federated learning is considered when there are more users overlapping and fewer features overlapping. This is consistent with our idea of the multi−dimensional information auction, which not only improves the performance of the server model but also performs experimental validation from the perspective of vertical federation learning in Section 4.

## 3. Theory of SecMDGM Mechanism for Federated Learning

As a distributed integration approach, federated learning has many advantages. How to make clients voluntarily submit higher−quality data or local computing performance is an important area of focus. We design an incentive mechanism named SecMDGM to facilitate federated learning tasks based on the theory of first−price auction. The use of multi−attribute auctions is intuitive, but it is essential to completely prove the theory since this allows us to do away with the theoretical system of the VCG model, given in definition 1. We need to improve the proof to ensure that such a mechanism is feasible and necessary. Since participants provide more and more private information, how can they reduce their worries about the information being leaked, even if they can theoretically get the best benefits? Moreover, whether the participants of multi−round federated learning will steal bid information from each other is also a security issue.

The multi−dimensional bid information of the auction is calculated in the score function, which is mentioned in Equation (4). It is important to ensure the security of the score function, which also protects the safety of the client's original private information. Due to the particularity of the federated learning task, the server is trusted by default, so participants only get the public key. Only the server has the corresponding private key.

This section of the paper looks at how to ensure that the score function of the server is not leaked, a security guarantee that needs to be achieved to ensure that the multi−dimensional bidding information of clients will not be leaked. In addition, this section will theoretically prove the necessity of the SecMDGM mechanism from the perspectives of Pareto optimality and incentive compatibility. This means that the mechanism can maximize the revenue of all parties.

### 3.1. Algorithms and Framework of the SecMDGM Mechanism

The SecMDGM mechanism is based on the theory of first−price auction, one of the fundamental theories for auction mechanism. The algorithms and framework in this subsection focus on steps 1 to 4 in Figure 1. We believe the model clustering for federation learning can be found in papers dedicated to the computation of federation learning.

The auction theory in this paper is based on multi−dimensional attributes, as shown in Equation (9), where $Q$ is the set of bidder features. We should pay attention not only to the bidding price but also to the data quality, computing performance, and other factors in bidding. Therefore, a scoring function Score($Q$, $p$) is needed to measure each feature, and each feature has its corresponding weight, which is mentioned in Equation (4). In other words, the auction's winner needs to be measured in multiple dimensions to win finally.

Equation (9) indicates the $m$ dimension feature the client $i$ needs to submit, and $Q$ denotes the feature array.

$$Q_i = (q_1, q_2, \cdots, q_m) \tag{9}$$

$$bid_{client\_i}\left(Encrypt_{pk_1}(Q), Encrypt_{pk_2}(p)\right) = \tag{10}$$

$$bid_{client_i}\left(Encrypt_{pk_1}(q_1), \cdots, Encrypt_{pk_1}(q_m), Encrypt_{pk_2}(p)\right)$$

Equation (10) indicates that client $i$ submits the feature array $Q$ and the bid price $p$ to the seller, which refers to the server. Moreover, since the seller has distributed the auction rules and the public keys to the buyers separately, as known in the first step shown in Figure 1, the clients need to encrypt their submitted bid information separately.

Figure 1 displays the overall framework of the SecMDGM mechanism, and the mechanism is divided into seven steps. The last steps of model aggregation are well known, and the first steps are the mechanism design that is the focus of this paper. Thanks to its inclusion, participants can actively participate in the training of the model, while the security of the data is guaranteed. Algorithm 1 provides the pseudo−code. This section provides the flow of the SecMDGM mechanism, and the next section analyzes in detail how this mechanism is realized and proved.

### 3.2. Cryptographic Utility and Score Functions for the SecMDGM Mechanism

The utility function is a commonly used measurement method in microeconomics, which is used to measure buyers' satisfaction when they consume an item. In this paper, it is the satisfaction of the server with the bidding information provided by the clients. This is a subjective feeling perception, so there are many different types of utility functions and the server determines the weights of the features.

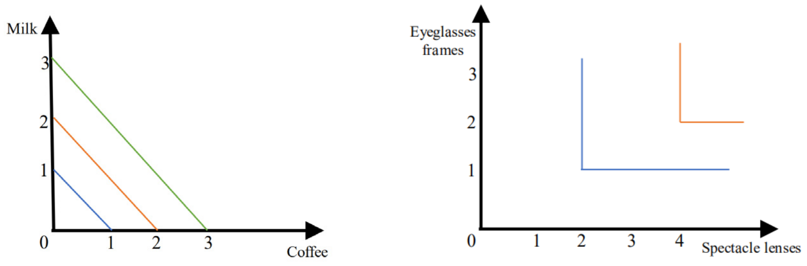
The indifference curve is used to show that items of two groups in different combinations can provide the same utility. The consumer's choice of any point on the curve is of equal utility to the consumer because the combination represented by any point provides the consumer with no difference in satisfaction. Hence, it is termed the utility's indifference curve. The multi−dimensional information in the bidding of clients is such a combination. We must ensure that it conforms to the federal learning requirements by giving the suitable utility function and the corresponding indifference curve.

**Algorithm 1:** Federated Learning Security Mechanism in Round $b$

```
Input: Number of clients: $N$;
       Number of participants in the last round: $K$;
       Local multi−dimensional data;
       Round $b - 1$.
Output: Global model parameter $\omega(t)$:
for $t$ = 1 to $T$ do
    $client_1$ to $client_N \leftarrow pk_1, pk_2$ and $Score(Q, p)$ rules
    for $i$ = 1 to $N$ do
        $Q_i \leftarrow$ arg max $U\ (Q_i) - c(Q_i, \theta_i)$ in Equation (17)
        $p\ _i \leftarrow c(Qi,\ \theta i) + \int_{\theta}^{\overline{\theta}} c_{\theta}(Q,t)(\frac{1-F(t)}{1-F(\theta)})^{N-1} dt$ in Equation (18)
        $E(Qi) \leftarrow$ encrypt with $pk_1$
        $E(pi) \leftarrow$ encrypt with $pk_2$
        submit $bid(E(Q_i), E(p_i))$
    end for
        $E(Score) \leftarrow\ E_{pk_1,\ pk_2}(U(q_1, \cdots, q_m) - p)$
    $Score \leftarrow\ \mathrm{D}_{sk_1,\ sk_2}(E(Score)$
    win$\leftarrow$ 0 or 1
    Add winner to round $b - 1$ for federated learning
    Complete the auction
    for $i$ = 1 to $K$ + 1 do
        $client_i \leftarrow pk_3, p\ _i$, global $\omega(t)$ from server
        $\omega_i(t\ +\ 1) \leftarrow$ trains the $client_i$
        server $\leftarrow E_{pk3}(\omega_i(t + 1))$
    end for
    $\omega(t + 1) \leftarrow \omega(t+1) = \frac{\sum_{i=1}^{N} C_i D_{sk_3} \omega_i(t+1)}{\sum_{i=1}^{N} C_i}$ in Equation (8)
end for
```

There are two typical forms of indifferentiable curves, the curve for perfect substitutes and the curve for perfect complements.

Take two items, for example. If a buyer wants to buy a thirst quencher when there are only two drinks to choose from, milk and coffee, then they are perfect substitutes, i.e., the buyer who buys milk will not buy coffee. As shown in Figure 5a, the three indifference curves represent the different demands for drinks. Equation (11) represents the utility function of the corresponding perfect substitutes.



(**a**) perfect substitutes curve (**b**) perfect complements curve

**Figure 5.** Indifference curve.

$$U(q_1, q_2) = \alpha_1 q_1 + \alpha_2 q_2 \tag{11}$$

If a buyer wants to buy eyeglasses, then lenses and frames are perfect complementary items because they must be presented together. As shown in Figure 5b, the two indifference curves represent the different demands for pairs of eyeglasses, respectively. Equation (12) represents the utility function of the corresponding perfect complements. In addition to the different results in the calculation of the utility function, the main difference between perfect substitutes and perfect complements is the different results in the marginal rates of substitution (MRS). The MRS for perfect substitutes is 0 (Equation (13)), and the latter result is ∞.

$$U(q_1, q_2) = \min(\alpha_1 q_1, \alpha_2 q_2) \tag{12}$$

$$MRS = -\frac{\Delta q_2}{\Delta q_1} \tag{13}$$

The multi−dimensional features of clients, such as CPU performance, memory capacity, hard disk capacity, network bandwidth, and other performance, can replace each other, so the perfect substitution utility function is suitable for calculating the multi−dimensional information in federated learning.

Figure 6 represents the perfect−substitution−type preference relationship (indifference curve) for three−dimensional features when $m$ is equal to three: $q_1$, $q_2$, and $q$. Figure 6 is an abstract description, so we do not consider the weight of each feature. We also do not need to consider the weights in the theoretical proof because they do not affect the proof of the mechanism design. The indifference curve means that for different combinations of features, all the points on the same surface have the same degree of utility for the server. This figure provides a better understanding of the utility function of the multi−dimensional auction.

The perfect substitution utility function has excellent theoretical support as a type of utility function. However, in federated learning, the training usually involves multiple rounds. In addition, the clients are generally not fixed, i.e., the auction is conducted in multiple rounds. To ensure that the multi−dimensional information of participants in different rounds is not leaked and the weights of the server are not leaked, we encrypted the perfect substitution utility function in Equation (14).

$$U(q_1, \cdots, q_m) = \alpha_1 q_1 + \alpha_2 q_2 + \cdots + \alpha_m q_m \tag{14}$$

$$= D_{sk_2}E_{pk_2}(\alpha_1 q_1) + E_{pk_2}(\alpha_2 q_2) + \cdots + E_{pk_2}(\alpha_m q_m)$$
$$= D_{sk_2}E_{pk_2}(D_{sk_1}(E_{pk_1}(\alpha_1) * E_{pk_1}(q_1)$$
$$= D_{sk_2}E_{pk_2}(D_{sk_1}(E_{pk_1}(\alpha_1) * E_{pk_1}(q_1) + E_{pk_2}\left(D_{sk_1}\left(E_{pk_1}(\alpha_2) * E_{pk_1}(q_2)\right)\right)$$
$$+ \cdots + E_{pk_2}\left(D_{sk_1}\left(E_{pk_1}(\alpha_m) * E_{pk_1}(q_m)\right)\right))$$

Equation (6) is the utility function of the security mechanism proposed in this paper. The server provides two public keys: $pk_1$ for the multiplication operation and $pk_2$ for the addition operation. Since the intermediate values after the encryption operation no longer contain the original plaintext data, their security is guaranteed.

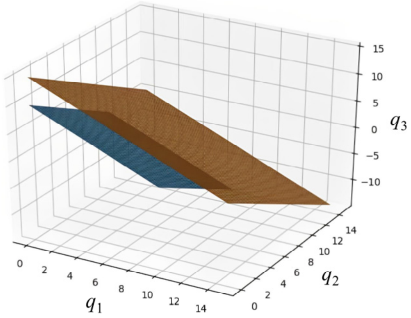


**Figure 6.** Three−dimensional indifference curve of the perfect substitution utility function.

The score function is Equation (15), which is the utility function minus the price $p$ submitted by the client when bidding. The following equation provides the encryption and decryption process of the scoring function, whose security guarantees are discussed in Section 2, so only its secure calculation process is shown here. The scoring function is used as part of the rules of the SecMDGM mechanism. Since we introduced the multi−dimensional information, a corresponding scoring function is needed to add as a supplement to the first−price auction rules.

$$\begin{aligned} Score_{client_i} &= U(q_{i_1}, \cdots, q_{i_m}) - p_i \\ &= D_{sk_2}E_{pk_2}(U(q_{i_1}, \cdots, q_{i_m}) - p_i) \\ &= D_{sk_2}E_{pk_2}(U(q_{i_1}, \cdots, q_{i_m})) - D_{sk_2}E_{pk_2}(p_i) \end{aligned} \quad (15)$$

The encrypted utility and scoring functions in this paper simultaneously ensure that (1) the communication process is secure when the client submits features and price to the server and (2) other malicious parties do not steal the parameters of the server when the auction is being executed. In addition, with these two functions, we developed scoring rules for multi−dimensional auctions. Sections 3.3 and 3.4 will prove that the mechanism discussed in this paper can be guaranteed in theory due to the introduction of the scoring function.

### *3.3. Maximize the Expected Profit of the SecMDGM Mechanism*

In this section, we prove the necessity of the SecMDGM mechanism to maximize the overall profit. This necessity is reflected in two aspects:

(1) The SecMDGM mechanism in this paper is based on multi−dimensional auction theory, which is more in line with the real auction of federated learning. Not only the price but also qualities are considered.

(2) An excellent mechanism enables the server to spend less but achieves a higher performance of the model. At the same time, all the participants are willing to submit more real data and local computing resources for the federated learning task to obtain higher profits.

The first point of necessity is intuition, and the higher the dimensionality of features, the higher the quality of the results. However, because of the introduction of the first point, we need more theory to ensure that the second point holds. We can measure the second point of necessity by the scoring function in the server, which is referred to in the previous section. The profit can be calculated by Equation (16). The profit is equal to the expected revenue given by the server minus the cost of the participation of the winner. The cost $c$ of the winner is related not only to the parameter $Q$ but also to the privacy parameter $\theta$.

$$profit(Q, p|\theta) = (p - c(Q, \theta)) * Prob(win|Score(Q, p)) \tag{16}$$

How can we design the incentive mechanism so that the two parties of federated learning maximize their profits? Submitting the real data of $Q$ and $p$ will be the optimal strategy. Equations (17) and (18) are the optimal bidding strategies. The proof is given below.

**Theorem 1.** *Maximize the Expected Profit from the SecMDGM Mechanism.*

$$Q_{winner} = argmaxU(Q) - c(Q, \theta) \tag{17}$$

$$p_{winner} = c(Q_{winner}, \theta) + \int_{\theta}^{\overline{\theta}} c_{\theta}(Q, t)\left(\frac{1-F(t)}{1-F(\theta)}\right)^{N-1} dt \tag{18}$$

**Proof of Theorem 1.** We use the reduction to absurdity to prove Equation (17).

Suppose that there is a dominant bidding strategy $bid(Q, p)$ in client $i$, who get the maximize maximum expected profit.

Contradiction: Exists another bidding strategy $bid(Q', p') \neq bid(Q, p)$, satisfies the following equations.

$$\begin{cases} Q' = argmaxU(Q') - c(Q', \theta') \\ p' = p + U(Q') - U(Q) \end{cases} \tag{19}$$

If the following conditions are satisfied, then the strict predominance of $bid(Q, p)$ is replaced by $bid(Q', p')$.

$$profit(Q', p'|\theta\prime) \geq \; profit(Q, p|\theta) \tag{20}$$

Transformation of Equation $p' = p + U(Q') - U(Q)$ can gets $U(Q) - p = U(Q') - p'$ and $Score(Q, p) = Score(Q', p')$. Since the scores are equal, then $Q' = Q = Q_{winner}$. This contradicts with $bid(Q', p') \neq bid(Q, p)$. Therefore, $Q' = argmaxU(Q\prime) - c(Q\prime, \theta\prime)\ holds$ and Equation (17) holds.

Equivalence Proof Equation (16): From the above, it is clear that once Equation (20) is proved then Equation (17) will hold.

$$profit(Q', p'|\theta') = (p' - c(Q', \theta')) * Prob(win|Score(Q', p')) \tag{21}$$

$$= (p - c(Q, \theta) + (U(Q') - c(Q', \theta') - ((U(Q) - c(Q, \theta)))) * Prob(win|Score(Q', p'))$$

$$\geq (p - c(Q, \theta)) * Prob(win|Score(Q', p'))$$

$$= profit(Q, p|\theta)$$

Therefore, Equation (20) holds, contradiction exists and Equation (17) holds.

The proof of Equation (18) is described in detail in articles [43,44], where $F()$ is the distribution function. Due to space limitations, it will not be repeated in this paper. Since the values of $Q$ and $p$ are the client's own strategy actions that are carried out locally before bidding, encryption is not required at this step. Therefore, the SecMDGM mechanism has the optimal strategies if the participants join the game. □

### 3.4. Pareto Optimal Mechanism and Incentive Compatibility (IC) of the SecMDGM Mechanism

Section 3.3 proved that the game has optimal strategies under the rules set by the SecMDGM mechanism, but it does not mean that the mechanism itself is optimal. In this section, we prove that the mechanism itself is optimal.

It is generally believed that the essential criteria to evaluate a mechanism include the effective allocation of resources and maximization of profit. Whereas efficient resource allocation needs to be demonstrated by proving Pareto optimality, maximizing profit must consider incentive compatibility. Therefore, we prove that the SecMDGM mechanism satisfies Pareto optimality and incentive compatibility.

**Theorem 2.** *Pareto Optimal of the SecMDGM Mechanism.*

The Pareto optimal mechanism can maximize the social surplus. It describes a state of optimal allocation of resources. There is no way to make it more profitable without causing losses to the other party.

**Proof of Theorem 2.** Equation is: $Surplus = U(Q) - c(q)$. Since Equation (17) has proved that in the optimal strategy, $Q_{winner} = argmaxU(Q) - c(Q, \theta)$.

These two equations are understood from different perspectives, but their results are the same, and we differ in obtaining the value of c from a global perspective, but since the mechanism proves Equation (17). The optimal strategy of the participants is to make the whole mechanism Pareto optimal. This means $Surplus$ can be the maximum when $Q = Q_{winner}$. Pareto Optimal of the SecMDGM Mechanism holds. □

**Theorem 3.** *Incentive Compatibility (IC) of the SecMDGM Mechanism.*

The federated learning mechanism allows clients to pursue their individual profits while maximizing collective profit. That means incentive compatible.

**Proof of Theorem 3.** If there exist clients who bid $bid(Q', p)$, where $\exists j, q_j > q_{j'}$. Equation (17) has proved that when $Q_{winner} = argmaxU(Q) - c(Q, \theta)$, the client can maximize the expected profit. From the utility function, it is known that $U(Q) > U(Q')$, and it is deduced that $Score(Q) > Score(Q')$. Thus, the winner that the mechanism chooses is the one that pursues their individual interests. □

The above two theorems show that the SecMDGM mechanism discussed in this paper can maximize the profit of both client and server and the client can actively submit more data and other multi−dimensional parameters, thus maximizing personal profit.

## 4. Experimental Verification of Federated Learning Security Mechanisms

To verify that the SecMDGM mechanism is not only secure and necessary but also effective, we simulate the federated learning process of the auction through experiments.

It is well known that algorithmic game theory can be divided into game strategy solving and mechanism design. Section 3.2 proves that the SecMDGM mechanism has the optimal game strategy. However, we focus on exploring the design of the mechanism so the experiments do not pursue the optimization of the game strategy but verify the effectiveness of the SecMDGM mechanism when the optimal solution has been proven.

Therefore, the weights of the score function are arbitrary and values will be given below. Suppose you want to reproduce the verification experiments to meet the rules of the SecMDGM mechanism. In that case, you can obtain some performance improvements of federated learning by using arbitrary values. Moreover, the features sought by each server are different, so the weight value is not essential.

In addition, no existing federal learning work can implement security mechanisms and multi−dimensional auctions. Therefore, the benchmark for this experiment is federal learning computing without a mechanism design in the same dataset.

To reduce the influence of the machine model on the results, the servers of this experiment are all based on the same operating system (Cents 7.9), which has the same performance as the Alibaba Cloud Server, with the same CPU model: Intel Xeon E5−2682 v4. The number of cores and memory capacity are taken as variables.

### *4.1. Data and Environment*

The model trained for the experiments is a logistic regression model, with a public dataset involving breast cancer, with 569 participants and 30 dimensions. The features are calculated from the digital image of a fine needle aspiration (FNA) of a breast mass. They describe the characteristics of the nucleus existing in the image. Table 1 provides a classification of this dataset.

**Table 1.** Dataset of breast cancer *.

| Classification | Number |
|---|---|
| Benign | 357 |
| Malignant | 212 |

* Retrieved from https://archive.ics.uci.edu/ml/datasets/Breast+Cancer+Wisconsin+%28Diagnostic%29, 29 November 2022.

As the multi−dimensional auction is perfectly consistent with the vertical data, this experiment is based on federal learning of vertical data and the features of the breast cancer dataset meet this requirement. As mentioned in the previous section, $Q = q_1 \cdots q_m$ denotes the multi−dimensional features submitted by clients. It can be CPU performance, memory capacity, number of local data users, number of local data features, etc.

In this experiment, we select two−dimensional features $Q = q_1, q_2$ for federated learning auctions and arbitrarily select $a_1 = 0.4, a_2 = 0.6$. As federated learning is usually a multi−round process, the multi−dimensional information of the client is important and should be encrypted. The security of encryption and decryption, as well as the steps in the auction mechanism, have been discussed in detail in the preceding sections. This section deliberately does not emphasize the encryption and decryption process but is completed under ciphertext.

To facilitate an intuitive presentation of the effectiveness of the SecMDGM mechanism in federated learning, the experiments began with round $b$ of bidding. In round $b - 1$, the accuracy of the logistic regression model was set to about 90% to reflect the improvement in the performance of different participants. In this experiment, $q_1$ denotes the performance of the client's computer, $q_2$ represents the number of features of local data, and $p$ represents the bid price. For the three features, we perform Min–Max normalization, which is shown in Equation (22), and complete the auction process in steps according to the specified parameter weights and auction rules of the SecMDGM mechanism.

$$q^{nor} = \frac{q - q^{min}}{q^{max} - q^{min}} \tag{22}$$

As shown in Table 2, after normalization, encryption, and decryption, using the perfect substitution utility and score function in Section 3, the highest scorer is the winner of this round of the first−price auction. Meanwhile, the winner needs to pay RMB 300 and provide 1VCPU 1Gib and 15−dimensional local data to participate in the model training. Therefore, client three can add to the training of the federated learning model.

**Table 2.** The *bth* bid for federated learning.

| Client | $q_1$ | $q_2$ | $p$ | Score | Win |
|---|---|---|---|---|---|
| 1 | 1vCPU 1Gib | 9 features | RMB 400 | −0.21 | 0 |
| 2 | 2vCPU 8Gib | 5 features | RMB 600 | −0.18 | 0 |
| **3** | **1vCPU 1Gib** | **15 features** | **RMB 300** | **0.04** | **1** |
| 4 | 1vCPU 4Gib | 10 features | RMB 350 | −0.01 | 0 |
| 5 | 1vCPU 4Gib | 5 features | RMB 400 | 0.34 | 0 |

The process of aggregation model of federated learning is also under encryption. To present the experimental results, the encryption and decryption processes are not emphasized in the experimental process. Figure 7 shows the flowchart of round *b* bidding, with five bidders and one winner. It is a partial diagram of Figure 1, which provides us with a more visual understanding of the local process of the experiment. Although the weights are chosen arbitrarily, the experimental data are from public datasets and the complete auction rules, cryptographic functions, and computational functions are provided. Thus, this is a reproducible experiment.

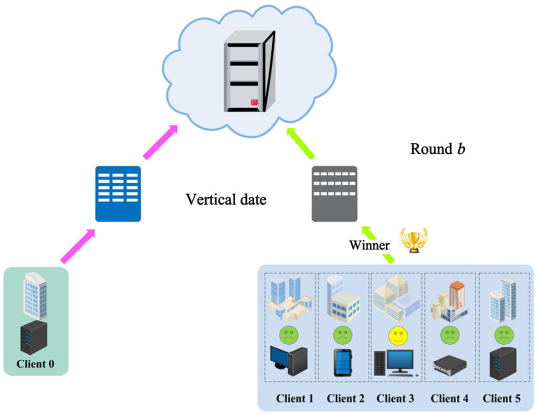


**Figure 7.** Two−dimensional auction in federated learning with vertical data.

### 4.2. Results and Analysis

Section 3 proves the security provided by and the necessity of the SecMDGM mechanism based on multi−dimensional auctions. This section corroborates that the SecMDGM mechanism can improve the model's accuracy by providing effective incentive to the five participants. Table 3 compares the work in this paper with state−of−the−art algorithms. We are the first to implement both the cryptographic mechanism and multi−dimensional auction in federated learning under vertical data. This is why we did not reproduce them in the experiments. On the basis of the baseline, we compare the winner and a random client under the SecMDGM mechanism.

**Table 3.** Comparison with state−of−the−art algorithms.

| | Mechanism Design | Encrypted Mechanism | Federated Learning | Encrypted Federated Learning | Vertical Data |
|---|---|---|---|---|---|
| Federated Avering [45] | | | √ | | |
| Pysyft [46,47] | | | √ | √ | |
| FMore [48] | √ | | √ | | |
| FATE [49] | | | √ | √ | √ |
| **This Paper** | **√** | **√** | **√** | **√** | **√** |

There are many different scenarios of federated learning. However, what remains limited is the budget funds and the number of participants on the server. The aim of the SecMDGM mechanism is to achieve a better model with less budget overhead, and we conduct model training on federated learning based on vertical data. The SecMDGM mechanism enables each client to participate actively. This can ensure a better model for the server and better profits for the client, and the multi−dimensional privacy features will not be leaked to other participants.

The baseline of this paper is the model in round $b-1$. To make the gap in the accuracy more apparent, we adjust the accuracy of the baseline to 90%. The experiments are compared by comparing random clients with the winner under the auction mechanism in round $b$, which can highlight the effectiveness of the SecMDGM mechanism.

Figure 8 shows the accuracy curves of the models with different participants. The accuracy of the models in round b is better than that of the models in round $b-1$, and the accuracy of the model for the winner is obviously better than that for a random client. This can highlight the effectiveness of the SecMDGM mechanism.

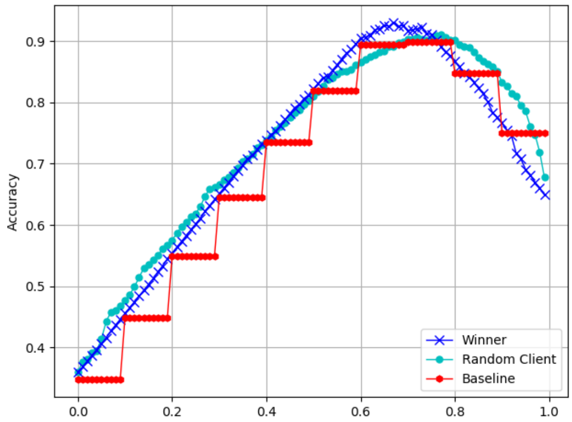


**Figure 8.** Accuracy for different participants.

More precisely, Figure 9 displays the improvement in the model accuracy by two different mechanisms. The SecMDGM mechanism is found to improve the model accuracy by nearly 3 times compared to that using the method of random clients. The optimal mechanism showed a more significant improvement than the random auction mechanism. The performance of the randomly selected client improved by about 1%, with almost no change. In contrast, for the aggregation model based on the vertical data, the performance of the winner improved by 2.73 times.

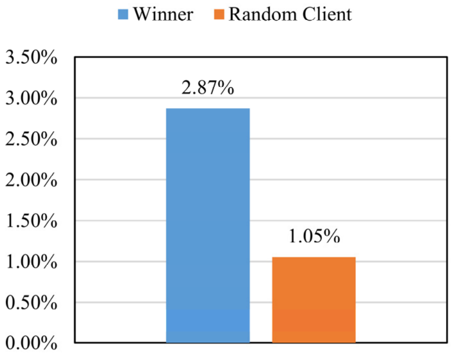


**Figure 9.** Increased accuracy of different participants.

Figure 10 shows the loss curves of different models. Due to more characteristic dimensions of the winner, its loss curve shows a more significant jump than others in the first few iterations. Moreover, it can converge quickly within a reasonable range, which is acceptable and reasonable.

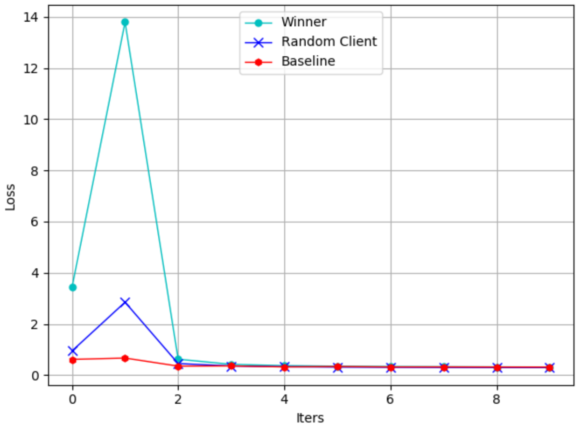


**Figure 10.** Loss for different participants.

The receiver operating characteristic (ROC) and the area under the ROC curve (AUC) are often used to measure the goodness of the model. The horizontal axis of the ROC curve is the FPR, and the vertical axis is the TPR. The larger the AUC, the better the model. Figure 11 shows that the winner model is better than the randomly selected client.

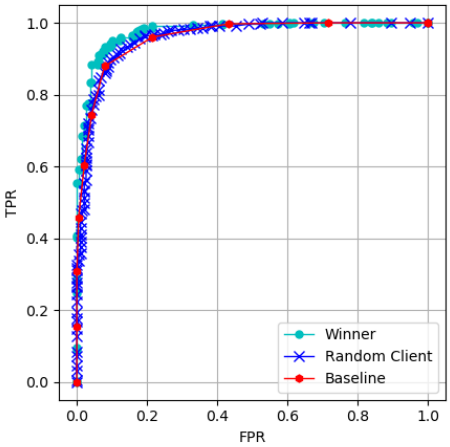


**Figure 11.** Graph of the ROC and the AUC.

As the experiment in this section only verifies the effectiveness of the design of the SecMDGM mechanism, the values of $m$ in $p_1$~$p_m$ and $a_1$~$a_m$ are far lower than in the real scenes. Nevertheless, they are sufficient to reflect the effectiveness of the SecMDGM mechanism.

The SecMDGM mechanism in federated learning is theoretically proved in Sections 2 and 3 and verified by experiments in Section 4. Therefore, the multi−dimensional secure federated learning mechanism in this paper is secure, necessary, safe, and effective. In future work, we can not only consider the mechanism but also discuss the optimal strategy of the game. We believe that this will lead to improved results.

## 5. Conclusions

There is no doubt about the importance of federated learning, and research has gradually focused on the security of the aggregation model. However, the issue is not only in the computation but also in motivating participants to join in the federated learning. In this paper, first, the multi−dimensional auction mechanism has been verified theoretically and experimentally to improve the performance of the model. However, federated learning participants often change, and the provided data and computational performance will dynamically change for fear of leaks. Second, security is considered to make multi−dimensional auctions more practical, and we solve this challenge by the partial homomorphic encryption scheme. Through theoretical proof and experimental verification, the security, necessity, and effectiveness of the SecMDGM mechanism are proved. However, the actual environment is more complex and changeable, and more difficult problems remain to be solved, such as multi−winner auctions and multi−dimensional incentive mechanisms with budget constraints, which need to be discussed in the future.

**Author Contributions:** Conceptualization, Q.C., L.Y. and X.W.; methodology, Q.C. and T.M.; software, Q.C. and Y.W.; validation, Z.L.J. and Y.W.; formal analysis, Q.C.; investigation, Q.C., L.Y. and X.W.; resources, Q.C., L.Y. and X.W.; data curation, Z.L.J.; writing—original draft preparation, Q.C.; writing—review and editing, Q.C., L.Y. and X.W.; visualization, Q.C.; supervision, L.Y. and X.W.; project administration, Q.C. and Z.L.J.; funding acquisition, Q.C. and Z.L.J. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by the Basic Research Project of Shenzhen, China (Nos. JCYJ20180507183624136 and JCYJ20200109113405927), the National Natural Science Foundation of China (Nos. 61872109 and 62272131), the National Science and Technology Major Project Carried on by Shenzhen (No. CJGJZD20200617103000001), the Guangdong Provincial Key Laboratory of Novel Security Intelligence Technologies (No. 2022B1212010005), the Science and Technology Project of Guangzhou (No. 2020A1515010652), Key Fields R&D Project of Guangdong Province (No. 2020B0101380001), and PINGAN-HITsz Intelligence Finance Research Center (No. YH-OAS-TICS-2020-00101).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** The data used to support the funding of this study are included within the article.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Yu, K.; Lin, L.; Alazab, M.; Tan, L.; Gu, B. Deep learning−based traffic safety solution for a mixture of autonomous and manual vehicles in a 5g−enabled intelligent transportation system. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 4337–4347. [CrossRef]
2. Alazab, M.; Macfarlane, K. Why Telegram Became the Go−To App for Ukrainians–Despite Being Rife with Russian Disinformation. *The Conversation 2022*. Available online: https://theconversation.com/why-telegram-became-the-go-to-app-for-ukrainians-despite-being-rife-with-russian-disinformation-179560 (accessed on 30 November 2022).
3. Sun, J.; Xu, G.; Zhang, T.; Alazab, M.; Deng, R.H. A practical fog−based privacy−preserving online car−hailing service system. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 2862–2877. [CrossRef]
4. Ebrahimpour, G.; Haghighi, M.S.; Alazab, M. Can blockchain be trusted in industry 4.0? study of a novel misleading attack on bitcoin. *IEEE Trans. Ind. Inform.* **2022**, *18*, 8307–8315. [CrossRef]
5. Yuan, J.; Jiang, Q.; Pan, Y. The influence mechanism of knowledge network allocation mechanism on knowledge distillation of high−tech enterprises. *Comput. Intell. Neurosci.* **2022**, *2022*, 1–18. [CrossRef] [PubMed]
6. Maddikunta, P.K.R.; Pham, Q. −V.; Prabadevi, B.; Deepa, N.; Dev, K.; Gadekallu, T.R.; Ruby, R.; Liyanage, M. Industry 5.0: A survey on enabling technologies and potential applications. *J. Ind. Inf. Integr.* **2022**, *26*, 100257.
7. Kattepur, A.; Khemkha, S. Aspects of mechanism design for industry 4.0 multi−robot task auctioning. *EAI Endorsed Trans. Smart Cities* **2022**, *6*, 1–13. [CrossRef]
8. Raphael, K.; Balaguer, J.; Tacchetti, A.; Weinstein, A.; Zhu, T.; Hauser, O.; Williams, D.; Campbell−Gillingham, L.; Thacker, P.; Botvinick, M.; et al. Human−centered mechanism design with democratic ai. *Nat. Hum. Behav.* **2022**, *6*, 1398–1407.
9. Voigt, P.; Von dem Bussche, A. *The EU General Data Protection Regulation (GDPR). A Practical Guide*, 1st ed.; Springer International Publishing: Cham, Switzerland, 2017; Volume 10, pp. 10–5555.
10. Thakur, P.S.; Kiran, U.; Sahu, O.P. *A Review on: Machine Learning Techniques to Mitigate Security Risks in IOT Framework State of the Art in Futuristic Communication and Network Technologies*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 671–679.
11. Yang, Q.; Liu, Y.; Chen, T.; Tong, Y. Federated machine learning: Concept and applications. *ACM Trans. Intell. Syst. Technol. (TIST)* **2019**, *10*, 1–19. [CrossRef]
12. Du, Z.; Wu, C.; Yoshinaga, T.; Yau, K.-L.A.; Ji, Y.; Li, J. Federated learning for vehicular internet of things: Recent advances and open issues. *IEEE Open J. Comput. Soc.* **2020**, *1*, 45–61. [CrossRef]

13. Sim, R.H.L.; Zhang, Y.; Chan, M.C.; Low, B.K.H. Collaborative machine learning with incentive−aware model rewards. In Proceedings of the International Conference on Machine Learning, Vienna, Austria, 12–18 July 2020; pp. 8927–8936.
14. Sarikaya, Y.; Ercetin, O. Motivating workers in federated learning: A stackelberg game perspective. *IEEE Netw. Lett.* **2019**, *2*, 23–27. [CrossRef]
15. Konecny, J.; McMahan, B.; Ramage, D. Federated optimization: Distributed optimization beyond the datacenter. *arXiv* **2015**, arXiv:1511.03575.
16. Alazab, M.; Rm, S.P.; Parimala, M.; Maddikunta, P.K.R.; Gadekallu, T.R.; Pham, Q. −V. Federated learning for cybersecurity: Concepts, challenges, and future directions. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3501–3509. [CrossRef]
17. Kandati, D.R.; Gadekallu, T.R. Genetic clustered federated learning for covid−19 detection. *Electronics* **2022**, *11*, 2714. [CrossRef]
18. Supriya, Y.; Tech, M.; Bindu, G.H.; Tech, M.; Reddy, K.D. Securing cloud data using identity−based encryption scheme under key exposure. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2018**, *3*, 807–814.
19. Javed, A.R.; Rehman, S.U.; Khan, M.U.; Alazab, M.; Reddy, T. Canintelliids: Detecting in−vehicle intrusion attacks on a controller area network using cnn and attention−based Gru. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 1456–1466. [CrossRef]
20. Zhan, Y.; Zhang, J.; Hong, Z.; Wu, L.; Li, P.; Guo, S. A survey of incentive mechanism design for federated learning. *IEEE Trans. Emerg. Top. Comput.* **2021**, *10*, 1035–1044. [CrossRef]
21. Wang, J.; Zhao, L.; Liu, J.; Kato, N. Smart resource allocation for mobile edge computing: A deep reinforcement learning approach. *IEEE Trans. Emerg. Top. Comput.* **2019**, *9*, 1529–1541. [CrossRef]
22. Von Neumann, J.; Morgenstern, O. *Theory of Games and Economic Behavior*; Princeton University Press: Princeton, NJ, USA, 2007.
23. Roughgarden, T. Algorithmic game theory. *Commun. ACM* **2010**, *53*, 78–86. [CrossRef]
24. Myerson, R.B. Mechanism design. In *Allocation, Information and Markets*; Springer: Berlin/Heidelberg, Germany, 1989; pp. 191–206.
25. Börgers, T.; Krahmer, D. *An Introduction to the Theory of Mechanism Design*; Oxford University Press: New York, NY, USA, 2015.
26. Nisan, N.; Ronen, A. Algorithmic mechanism design. *Games Econ. Behav.* **2001**, *35*, 166–196. [CrossRef]
27. Yang, P.; Yan, S.; Zhu, D.; Wang, J.; Wu, F.; Yan, Z.; Yan, S. Improved sparrow algorithm based on game predatory mechanism and suicide mechanism. *Comput. Intell. Neurosci.* **2022**, *2022*, 1–23. [CrossRef]
28. Murali, M.; Thyagarajan, K.; Reddy, K.D. Document clustering for digital devices: An approach to improve forensic analysis. *Int. J. Eng. Res. Manag. Technol.* **2014**, *1*, 208–212.
29. Vickrey, W. Counterspeculation, auctions, and competitive sealed tenders. *J. Financ.* **1961**, *16*, 8–37. [CrossRef]
30. Shen, W.; Peng, B.; Liu, H.; Zhang, M.; Qian, R.; Hong, Y.; Guo, Z.; Ding, Z.; Lu, P.; Tang, P. Reinforcement mechanism design: With applications to dynamic pricing in sponsored search auctions. *AAAI Conf. Artif. Intell.* **2020**, *34*, 2236–2243. [CrossRef]
31. Choi, H.; Mela, C.F.; Balseiro, S.R.; Leary, A. Online display advertising markets: A literature review and future directions. *Inf. Syst. Res.* **2020**, *31*, 556–575. [CrossRef]
32. Lebrun, B. Existence of an equilibrium in first price auctions. *Econ. Theory* **1996**, *7*, 421–443. [CrossRef]
33. Ion, M.; Kreuter, B.; Nergiz, A.E.; Patel, S.; Saxena, S.; Seth, K.; Raykova, M.; Shanahan, D.; Yung, M. On deploying secure computing: Private intersection−sum−with−cardinality. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy (EuroS&P), Genoa, Italy, 7–11 September 2020; pp. 370–389.
34. Walker, A.; Patel, S.; Yung, M. Helping Organizations Do More without Collecting More Data. Google Security Blog. 2019. Available online: https://security.googleblog.com/2019/06/helping-organizations-do-more-without-collecting-more-data.html (accessed on 29 November 2022).
35. McAfee, R.P.; McMillan, J. Auctions and bidding. *J. Econ. Lit.* **1987**, *25*, 699–738.
36. Laffont, J. −J.; Ossard, H.; Vuong, Q. Econometrics of first−price auctions. *Econom. J. Econom. Soc.* **1995**, *63*, 953–980.
37. Grundl, S.; Zhu, Y. Robust Inference in First−Price Auctions: Overbidding as an Identifying Restriction. Finance and Economics Discussion 2019, 1–51. Available online: https://www.sciencedirect.com/science/article/abs/pii/S0304407622001221 (accessed on 29 November 2022).
38. Bichler, M. An experimental analysis of multi−attribute auctions. *Decis. Support Syst.* **2000**, *29*, 249–268. [CrossRef]
39. Acar, A.; Aksu, H.; Uluagac, A.S.; Conti, M. A survey on homomorphic encryption schemes: Theory and implementation. *ACM Comput. Surv.* **2018**, *51*, 1–35. [CrossRef]
40. Mahajan, P.; Sachdeva, A. A study of encryption algorithms AES, des and RSA for security. *Glob. J. Comput. Sci. Technol.* **2013**, *13*, 15–22.
41. Paillier, P. Public−key cryptosystems based on composite degree residuosity classes. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Prague, Czech Republic, 2–6 May 1999; Springer: Berlin/Heidelberg, Germany, 1999; pp. 223–238.
42. Hard, A.; Rao, K.; Mathews, R.; Ramaswamy, S.; Beaufays, F.; Augenstein, S.; Eichner, H.; Kiddon, C.; Ramage, D. Federated learning for mobile keyboard prediction. *arXiv* **2018**, arXiv:1811.03604.
43. Che, Y.-K. Design competition through multidimensional auctions. *RAND J. Econ.* **1993**, *24*, 668–680. [CrossRef]
44. Riley, J.G.; Samuelson, W.F. Optimal auctions. *Am. Econ. Rev.* **1981**, *71*, 381–392.
45. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; Arcas, B.A.Y. Communication−efficient learning of deep networks from decentralized data. In *Artificial Intelligence and Statistics*; PMLR: Fort Lauderdale, FL, USA, 2017; pp. 1273–1282.
46. Ryffel, T.; Pointcheval, D.; Bach, F.; Dufour−Sans, E.; Gay, R. Partially encrypted deep learning using functional encryption. *Adv. Neural Inf. Process. Syst.* **2019**, *32*, 4519–4530.

47. Ryffel, T.; Trask, A.; Dahl, M.; Wagner, B.; Mancuso, J.; Rueckert, D.; Passerat−Palmbach, J. A generic framework for privacy preserving deep learning. *arXiv* **2018**, arXiv:1811.04017.
48. Zeng, R.; Zhang, S.; Wang, J.; Chu, X. Fmore: An incentive scheme of multi−dimensional auction for federated learning in MEC. In Proceedings of the 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), Singapore, 8–10 July 2020; pp. 278–288.
49. Yang, Q.; Liu, Y.; Cheng, Y.; Kang, Y.; Chen, T.; Yu, H. Federated learning. *Synth. Lect. Artif. Intell. Mach. Learn.* **2019**, *13*, 1–207.