IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 18, 2019, accepted September 6, 2019, date of publication September 12, 2019,
date of current version September 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2940714

Regression Analysis With Differential Privacy Preserving

XIANJIN FANG[1], FANGCHAO YU[1], GAOMING YANG[1], AND YOUYANG QU[2]
[1]School of Computer Science and Engineering, Anhui University of Science and Technology, Huainan 232000, China
[2]School of Information Technology, Deakin University, Burwood, VIC 3156, Australia

Corresponding author: Gaoming Yang (gmyang@aust.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61572034, in part by the Major Science and Technology Projects in Anhui Province under Grant 18030901025, and in part by the Anhui Province University Natural Science Fund under Grant KJ2019A109.

ABSTRACT In the field of data mining, protecting sensitive data from being leaked is part of the focuses of current research. As a strict and provable definition of privacy model, differential privacy provides an excellent solution to the problem of privacy leakage. Numerous methods have been suggested to enforce differential privacy in various data mining tasks, such as regression analysis. However, existing solutions for regression analysis is less than satisfactory since the amount of noise added is excessive. What's worse, the adversary can launch model inversion attacks to infer sensitive information with the published regression model. Motivated by this, we propose a differential privacy budget allocation model. We optimize the regression model by adjusting the privacy budget allocation within the objective function. Extensive evaluation results show the superiority of the proposed model in terms of noise reduction, model inversion attack proof, and the trade-off between privacy protection and data utility.

INDEX TERMS Machine learning, differential privacy, regression analysis, model inversion attack.

I. INTRODUCTION

Regression analysis [1] is widely used in the fields of statistical analysis and data mining. For example, a medical institution collects a large number of clinical data of cancer patients. Researchers use regression analysis technology to analyze these data and build a model that can predict the risk of cancer. The medical institution publishes the model, and users can submit individual clinical data to the model to predict cancer risk. However, the privacy leakage issue [2] has not been well-considered in the regression analysis. On the one hand, the adversary can infer the sensitive information about the training set by combining the published regression model and some background knowledge. One the other hand, the ability of the regression model to discover the potential relationship between the data also provides an opportunity for the adversary to obtain sensitive information. Especially in medical, financial and other high-confidential fields, sensitive information in regression-based applications is under great threats.

To solve the problem of privacy leakage in regression analysis, various solutions have been proposed. On the data level, data masking is a common privacy protection mechanism, which achieves privacy by perturbation, encryption or generalization to datasets [3]–[6]. We can use the masking data to build the regression model, but it is challenging to achieve the balance between data privacy and model availability [7]. On the algorithm level, it is the research hotspot to build the regression model with privacy protection. For example, the regression model based on differential privacy [8] or homomorphic encryption [9]–[11]. Consideration of computing power and application scenarios, differential privacy is a better solution in many cases.

As a strict and provable definition of privacy model, differential privacy provides a method for quantitative evaluation of privacy protection and develops a new solution to the problem of privacy leakage in regression analysis. The core idea of the regression analysis with differential privacy is to add controllable noise to the regression model [12], which can ensure a balance between privacy preservation and utility.

There are two main methods to achieve differential privacy in regression analysis algorithm. The first method is directly injecting noise into the learned regression model [13]. It separates noise addition from the training process of the model, and ignores the relationship between model parameters and noise. This approach may lead to sizeable noise and reduce the utility of the prediction result. The second method is the objective perturbation mechanism [14]. Unlike the

The associate editor coordinating the review of this manuscript and approving it for publication was Nikhil Padhi.

former one, it adds noise to the objective function of the regression model and trains the regression model by the objective function after noise addition. In the optimization process, the noise-added model can minimize the interference caused by noise and improve the fitting effect. This approach is advanced at present.

Generally, the function mechanism [15], which is based on objective perturbation, performs better than other approaches in the field of regression analysis with differential privacy. In order to solve new problems and adapt to new application scenarios, we need to make some improvements to the function mechanism. Firstly, function mechanism never considers the difference in sensitivity of each part of the objective function. Therefore, it may result in uneven distribution of the internal privacy budget. In this case, the noise of the function mechanism is not optimized to a greater extent. Although, Gong *et al.* [16] proposed PrivR based on the function mechanism, which perturbs the polynomial coefficients according to the magnitude of relevance between the input features and the model output. However, the algorithm is complicated in the case of high-dimensional features. Secondly, model inversion attack [17] puts the function mechanism in great risks. The adversary can use the released regression model and some background knowledge to predict the target's sensitive attribute, which used as input to the model. Function mechanism can only protect regression model against model inversion attack when the privacy budget is small enough. It means the reduction of utility for the regression model. Wang *et al.* [18] makes some improvements. However, the algorithm is inflexible and the defense capability needs to be strengthened. Therefore, a private preservation framework that can significantly promote the data privacy while improving the accuracy in regression analysis is required urgently.

In order to solve the aforementioned issues, we present an algorithm named Differentiated Privacy Budget Allocation (DPBA). We consider the effect of sensitivity among various components in the objective function and allocate privacy budgets in accordance with sensitivity. We can optimize the model by adjusting the allocation of privacy budget. Compared with the previously mentioned solutions, the proposed algorithm is more flexible. Moreover, DPBA increases randomness of the algorithm, it can significantly decrease the risks of model inversion attacks. To summarize, we make the following contributions.

1) we propose DPBA, a new solution for differential privacy preserving in regression analysis. It provides improvement to allocate privacy budget. Compared with the previous, our method is more flexible and simple. At the same time, it shows good performance in privacy and utility of regression models.
2) Using DPBA, we can defend model inversion attacks. Compared with defense mechanism proposed by Wang *et al.* [18], our method is easy to implement and can achieve the better defensive capability.

TABLE 1. Definition of related symbols.

Symbol	Definition
$t_i = (x_i, y_i)$	the i-th tuple of data set
$f(t_i, \omega)$	the cost function of t_i
$f_D(\omega)$	$f_D(\omega) = \sum_{t_i \in D} f(t_i, \omega)$
ω^*	$\omega^* = argmin_\omega f_D(\omega)$
$f_D^*(\omega)$	the objective function after perturbation
$\phi(\omega)$	a product of elements in $\omega_1, \omega_2, ..., \omega_d$
$\Phi(\omega)$	the combination of the elements in ϕ
$\lambda_{\phi t_i}$	the coefficient of ϕ in $f(t_i, \omega)$

The remainder of the paper is organized as follows. Section II reviews related work of security and privacy in regression analysis. Section III introduces some basic concepts about this paper. Section IV explains our methods in detail. Section V conducts some comparative experiments to test the performance of our method. Finally, Section VI concludes the paper with directions for future work.

II. RELATED WORK

Security and privacy risks in regression analysis have attracted much attention. This section mainly introduces the related work of regression analysis with differential privacy and security threats in regression analysis. Table 1 shows the description of related symbols.

A. REGRESSION ANALYSIS WITH DIFFERENTIAL PRIVACY

As a strict and provable framework of privacy protection, differential privacy is widely employed [19]–[23]. In this paper, we mainly discuss regression analysis with differential privacy. Its main idea is to add appropriate noise to the regression model. Chaudhuri *et al.* [14] proposed objective perturbation mechanism. It achieves differential privacy by adding noise to the means of the objective function in the regression model. This mechanism is useful to reduce noise in the process of building the regression model. However, it is only suitable for linear regression. Kifer *et al.* [24] made some improvements in objective perturbation mechanism and generalized it to the regression analysis of high dimensional space. Besides, the problem of empirical risk minimization of regression models in high dimensional space is also discussed. However, it also can not apply to other regression methods except linear regression. Zhang *et al.* [15] presented the function mechanism based on objective perturbation mechanism, which is suitable for both linear regression and logistic regression. Function mechanism never directly adds noise to the objective function. First, It decomposes the objective function into polynomials. Then, it adds noise to each coefficient of the monomial term. Function mechanism shows good performance in generalization and privacy. In a recent study, Dwork and Feldman [25] also made some progress in the field of differential privacy regression analysis. They focus on the

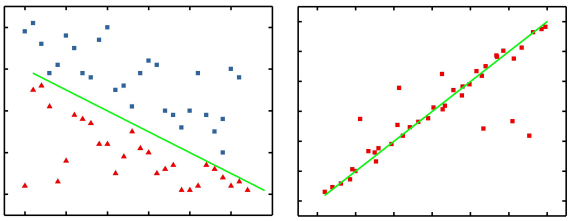


FIGURE 1. Logistic regression and linear regression.

convex optimization regression model. However, most of the research in regression analysis with differential privacy focus on the construction of parametric models. In addition, some researchers designed the non-parametric model, such as histogram publishing [26], [27] and gaussian process regression [28], [29]. In some specific scenarios, they can also have a good performance.

B. SECURITY THREATS IN REGRESSION ANALYSIS

Generally speaking, existing attacks against regression analysis can be classified into four categories: poisoning attacks [30], [31], evasion attacks [32], inference attacks [33], model stealing attacks [34]. In poisoning attacks, the adversary aims to produce a bad classifier by polluting the training dataset. The key to defending such attacks is to identify malicious samples in training sets. In evasion attacks, attackers aim to construct adversarial examples to bypass the classifier based on the regression model. Improving model robustness is critical to against such attacks. Inference attacks and model stealing attacks, the adversary's goal is to infer sensitive information about models or training data. Model perturbation is a common method to defend these two kinds of attacks. As we know, there is little research on the defense of various attacks at present. This paper focuses on model inversion attack, which is one of the inference attacks. Wang *et al.* [18] proposed a method of disturbing sensitive attributes in the cost function to defend model inversion attack. However, the defense capability of this method is limited. We need to build a regression model with more powerful defense capabilities.

III. PRELIMINARY

In this section, we introduce the concepts of regression model, differential privacy and model inversion attack.

A. REGRESSION MODEL

Let D be a data set that contains n tuples $t_1, t_2, \ldots, t_n$, each tuple includes $d+1$ explanatory attributes $X_1, X_2, \ldots, X_d, Y$, so $t_i = (x_{i1}, x_{i2}, \ldots, x_{id}, y_i)$, and $\sqrt{\sum_{i=1}^{d} x_{id}^2} \leq 1$. We set Y as the prediction result of the regression, and $X_1, X_2, \ldots, X_d$ as the input of the training model and prediction. In these individual attributes, X_s is the sensitivity attribute which is the target in model inversion attack. The regression model is shown in Fig.1.

Definition 1 (Linear Regression): Assume Y in data set D has a value range $[-1, 1]$. A linear regression on D returns a prediction function $p(x_i, \omega^*) = x_i^T \omega^*$, where ω^* is a d-dimensional real vector that minimizes the cost function $f_D(\omega)$.

$$f_D(\omega) = \sum_{i=1}^{n} (y_i - x_i^T \omega)^2 \tag{1}$$

$$\omega^* = argmin_\omega \sum_{i=1}^{n} (y_i - x_i^T \omega)^2 \tag{2}$$

Definition 2 (Logistic Regression): Assume Y has a value range $\{0, 1\}$. A logistic regression on D returns a prediction function which returns $\widehat{y_i} = 1$ with the probability $p(x_i, \omega^*) = \exp(x_i^T \omega^*)/(1 + \exp(x_i^T \omega^*))$, where ω^* is a d-dimensional real vector that minimizes cost function $f_D(\omega)$.

$$f_D(\omega) = \sum\nolimits_{i=1}^{n} (\log(1 + \exp(x_i^T \omega)) - y_i x_i^T \omega) \tag{3}$$

$$\omega^* = \arg\min_\omega \sum\nolimits_{i=1}^{n} (\log(1 + \exp(x_i^T \omega)) - y_i x_i^T \omega) \tag{4}$$

B. DIFFERENTIAL PRIVACY

Definition 3 (ϵ-Differential Privacy [12]): A randomized algorithm K satisfies ϵ-differential privacy, if any output S of K and for any two neighbor databases D_1 and D_2, we have

$$\Pr[K(D_1) \in S] \leq e^{\epsilon} \times \Pr[K(D_2) \in S]. \tag{5}$$

In definition 3, neighbor databases D_1 and D_2 represent two similar data sets that differ in one tuple. $\Pr[K(D_1) \in S]$ means the probability of $K(D_1) \in S$. The parameter ϵ is the privacy protection budget specified by the algorithm designer. In practical applications, ϵ takes a small value, such as 0.01, 0.1, or 1, etc. The smaller value of ϵ, the higher the differential privacy protection level rises.

Theorem 1 (Sequence Composition [12]): For algorithm $K_1, K_2, \ldots, K_n$, each privacy budget is $\epsilon_1, \epsilon_2, \ldots, \epsilon_n$, D is a data set, so $K(K_1(D), K_2(D), \ldots, K_n(D))$ satisfies $(\sum_{i=1}^{n} \epsilon_i)$-differential privacy.

C. GLOBAL SENSITIVITY

For algorithms based on differential privacy, it is critical to add reasonable volume of noise. On the one hand, if the added noise is not significant, the adversary can analyze the noise distribution to achieve the malicious purpose. On the other hand, if the added noise is too large, the output from the query seriously deviates from the true value. Therefore, we introduce the concept of sensitivity which refers to the maximum change caused by the deletion of any record in the data set. It is the key to measure the size of noise. The global sensitivity is a property of the function, and independent of the data set.

Definition 4 (Global Sensitivity [12]): Suppose D and D' are neighbor data sets, the global sensitivity of a function $f : D \to R^d$ is as follow,

$$\Delta f = \max_{D,D'} \left\| f(D) - f\left(D'\right) \right\|_1. \tag{6}$$

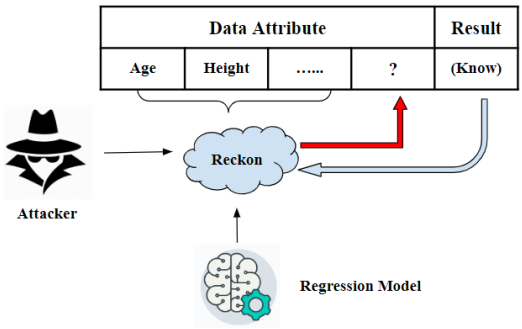


FIGURE 2. Attack model of model inversion attack.

D. NOISE MECHANISM

For differential privacy algorithm, the two mainstream mechanisms for adding noise includes laplace mechanism [13] which is mainly used to add noise to numerical results, and exponential mechanism [35] which is mainly used to add noise to discrete results. In this paper, we use numeral data as an instance and thereby we only leverage laplace mechanism. Laplace mechanism implements differential privacy protection by adding random noise that satisfies the Laplace distribution to the model. Assuming that parameter b satisfies laplace distribution, the probability density function is

$$p(x) = \frac{1}{2b}\exp(-\frac{|x|}{b}). \tag{7}$$

Theorem 2 (Laplace Mechanism [12]): An algorithm K takes a data set D, and $\epsilon > 0$, a query function $f : D \to R^d$ which sensitivity is Δf as input, and outputs as formula (8) where Q is noise satisfied Lap($\Delta f/\epsilon$). The algorithm K provides ϵ-differential privacy protection. if

$$K(D) = f(D) + Q. \tag{8}$$

The definition shows that the size of noise for laplace mechanism is determined by the sensitivity Δf and privacy budget ϵ. The sensitivity is determined by the query function. Once the query function is determined, the sensitivity is fixed, while the amount of noise added is determined by the privacy budget. The privacy budget increases with the decreasing of noise size.

E. MODEL INVERSION ATTACK

Model inversion attack arises from medical data protection of pharmacogenetics. Fredrikson *et al.* [17] proposed this attack model which can cause privacy leakage. Assuming that a research organization released a regression model $y = \rho(x, \omega^*)$ trained from a dataset D which contains the sensitive attribute X_s. An adversary acquires medical statistics which is similar to D, but some individual's sensitive attribute X_s is unknown. Combined with some background knowledge about individuals and the regression model, the adversary can obtain the sensitive attribute values by model inversion attack. The attack model is shown in Fig.2.

For the regression model with differential privacy, model inversion attack still puts sensitive information under great threats. We can defeat the attack when the privacy budget is small. However, the smaller of the privacy budget causes the worse availability of regression model.

IV. DIFFERENTIAL PRIVACY BUDGET ALLOCATION MODELING AND ANALYSIS

A. SYSTEM MODELING

In the function mechanism [15], Zhang reorganizes the cost function of regression model, and adds noise satisfied laplace distribution to each coefficient of monomial term $\phi(\omega)$,which include ω.

$$f_D(\omega) = \sum_{t_i \in D} f(t_i, \omega) = \sum_{j=1}^{J} \sum_{\phi \in \Phi_j} \sum_{t_i \in D} \lambda_{\phi t_i} \phi(\omega) \tag{9}$$

Generally, we assume $f_D(\omega)$ as an objective function of the regression model, where sensitivity is Δf and privacy budget is ϵ. In the function mechanism, converting $f_D(\omega)$ to the polynomial is the basic idea. Firstly, it set $f_D(\omega) = a\omega^2 + b\omega + c$, which a and b represent the coefficients of the objective function and c is a constant term. Next, it adds noise $Lap(\Delta f/\epsilon)$ which satisfies the laplace distribution to the coefficients of the monomial containing ω, the objective function after noise injection is

$$f_D^*(\omega) = (a + Lap(\Delta f/\epsilon))\omega^2 + (b + Lap(\Delta f/\epsilon))\omega + c.$$

After calculating gradient descent, optimal model ω^* will be obtained. The problem of the function mechanism is that it adds same amount of noise to all the coefficients of the monomial term containing ω, and does not consider the difference of sensitivity between monomial terms. As a result, the amount of added noise is more than expectation, because different sensitivity of monomial terms have different degrees of influence on the objective function.

In order to solve this problem, the influence of each monomial term to objective function should get consideration. In this case, we can combine the composition characteristic of differential privacy to make improvements to the function mechanism. The composition characteristic points out that multiple combinations of an algorithm which satisfies the differential privacy still meets the requirements of differential privacy. In this paper, we propose a solution based on the composition characteristic of differential privacy and the function mechanism.

Let $g_D(\omega) = a\omega^2$, $h_D(\omega) = b\omega$. The sensitivity of $g_D(\omega)$ is Δf_1 and the sensitivity of $h_D(\omega)$ is Δf_2, and $f_D(\omega) = a\omega^2 + b\omega + c$. Moreover, for a regression model without considering c, we have $\Delta f = \Delta f_1 + \Delta f_2$. The improved idea is to decompose the polynomial of the objective function into monomial terms, and assign different privacy budgets according to the sensitivity of the monomial term. We suppose the privacy budget allocated to $g_D(\omega)$, $h_D(\omega)$ is ϵ_1 and ϵ_2, $\epsilon_1 + \epsilon_2 = \epsilon$. After adding noise to $g_D(\omega)$ and $h_D(\omega)$, $g_D^*(\omega) = (a+Lap(\Delta f_1/\epsilon_1))\omega^2$, $h_D^*(\omega) = (b+Lap(\Delta f_2/\epsilon_2))\omega$, so

$$f_D^*(\omega) = g_D^*(\omega) + h_D^*(\omega) + c$$
$$f_D^*(\omega) = (a + Lap(\Delta f_1/\epsilon_1))\omega^2 + (b + Lap(\Delta f_2/\epsilon_2))\omega + c$$

Finally, using gradient descent to $f_D^*(\omega)$, we can obtain the optimal regression model. The algorithm is shown as Algorithm 1.

This algorithm use α and β as a variable to adjust the value of ϵ_1 and ϵ_2. By adjusting the values of ϵ_1 and ϵ_2, we can get a more optimized regression model. In this way, we optimize the distribution of the internal privacy budget of the objective function, and ensure less noise is added to the target function. At the same time, this uneven noise addition method also makes the regression model effective against model inversion attacks.

Algorithm 1 Differentiated Privacy Budget Allocation

Input: Privacy budget ϵ, data set D,objective function $f_D(\omega)$
Output: Optimal model ω^*
if linear regression **then**
  expanding the objective function $f_D(\omega)$ to polynomial
  set $g_D(\omega) = \sum_{1\le j,l\le d}(\sum_{t_i\in D} x_{ij}x_{il})\omega_i\omega_j$
  set $h_D(\omega) = \sum_{j=1}^{d}(2\sum_{t_i\in D} y_i x_{ij})\omega_j$
else if logistic regression **then**
  expanding the objective function $f_D(\omega)$ to polynomial
  set $g_D(\omega) = \frac{1}{8}\sum_{i=1}^{n}(x_i^T)^2\omega^2$
  set $h_D(\omega) = (\frac{1}{2}\sum_{i=1}^{n} x_i^T - \sum_{i=1}^{n} y_i x_i^T)\omega$
end if
compute the sensitivity of $g_D(\omega)$, $h_D(\omega)$ as Δf_1 and Δf_2
set the coefficient of $g_D(\omega)$, $h_D(\omega)$ as a and b
if $\Delta f_1 > \Delta f_2$ **then**
  set $\alpha = \frac{\Delta f_1}{(\Delta f_1)^2+\Delta f_2}\beta, 0 < \beta < \frac{f_2}{f_1} + f_1$
else
  set $\alpha = \frac{\Delta f_1}{(\Delta f_2)^2+\Delta f_1}$
end if
set $\epsilon_1 = \alpha\epsilon, \epsilon_2 = \epsilon - \epsilon_1$
compute $g_D^*(\omega) = (a + Lap(\Delta f_1/\epsilon_1))\omega^2$
compute $h_D^*(\omega) = (b + Lap(\Delta f_2/\epsilon_2))\omega$
set $f_D^*(\omega) = g_D^*(\omega) + h_D^*(\omega)$
compute $\omega* = \arg\min_\omega f_D^*(\omega)$
return ω^*

B. ALGORITHM OVERVIEW

In this section, we introduce the main steps of the algorithm in details. Due to the difference in objective function between linear regression and logistic regression, so we deal with them differently. In the first step of the algorithm, we need to identify the types of models, linear regression or logistic regression. It depends on the type of task we are dealing with. According to the models, we determine the objective function as in function mechanism and split it to $g_D(\omega)$ and $h_D(\omega)$. Then, we need to calculate the sensitivity Δf_1, Δf_2 of $g_D(\omega)$ and $h_D(\omega)$. The allocation of privacy budget is determined by sensitivity. we tend to allocate more privacy budgets to more sensitive items, because the greater the sensitivity, the greater the impact on the model. We use more privacy budgets to reduce the amount of noise. In general, we set $\beta = max(\Delta f_1, \Delta f_2)$. When $\Delta f_1 > \Delta f_2$, $\alpha = \frac{(\Delta f_1)^2}{(\Delta f_1)^2+\Delta f_2}$, so $\epsilon_1 = \frac{(\Delta f_1)^2}{(\Delta f_1)^2+\Delta f_2}\epsilon$. The range of noise added for $g_D(\omega)$ is $\Delta f_1/\epsilon_1 = \frac{\Delta f_1}{\epsilon} + \frac{\Delta f_2}{\Delta f_1\epsilon}$. In the function mechanism, the added noise for $g_D(\omega)$ is $\frac{\Delta f_1}{\epsilon} + \frac{\Delta f_2}{\epsilon}$. So, we reduce the noise of the more sensitive items. When total privacy budget ϵ is small or d is so big (high-dimensional feature of dataset) and other specific requirements scenarios, we can make appropriate adjustments to β. After that, the value ϵ_1 and ϵ_2 are obtained. Next, we add noise to the coefficient of $g_D(\omega)$ and $h_D(\omega)$ and compose a new cost function. Finally, computing $\omega* = \arg\min_\omega f_D^*(\omega)$, we can get the optimal regression model.

C. SYSTEM ANALYSIS

Lemma 1: The objective function of regression model is $f_D(\omega) = g_D(\omega) + h_D(\omega) + c$. The sensitivity of the objective function $f_D(\omega)$without considering c is Δf, and the sensitivity of $g_D(\omega)$, $h_D(\omega)$ is Δf_1 and Δf_2, then $\Delta f = \Delta f_1 + \Delta f_2$.

Proof: In function mechanism [15], Zhang proposed a method for computing the sensitivity of the objective function. Let D and D' be any two neighbor databases, and $f_D(\omega)$ and $f_{D'}(\omega)$ be the objective functions of regression analysis on D and D', respectively.

$$f_D(\omega) = \sum_{j=1}^{J}\sum_{\phi\in\Phi_j}\sum_{t_i\in D}\lambda_{\phi t_i}\phi(\omega)$$

$$f_{D'}(\omega) = \sum_{j=1}^{J}\sum_{\phi\in\Phi_j}\sum_{t_i'\in D'}\lambda_{\phi t_i'}\phi(\omega)$$

Then, we can get the following inequality

$$\sum_{j=1}^{J}\sum_{\phi\in\Phi_j}\left\|\sum_{t_i\in D}\lambda_{\phi t_i} - \sum_{t_i'\in D'}\lambda_{\phi t'}\right\|_1 \le 2\max_t\sum_{j=1}^{J}\sum_{\phi\in\Phi_j}\left\|\lambda_{\phi t}\right\|_1$$

This inequality is useful for our proof. First, we present the proof in the linear regression model with differential privacy. The objective function of a linear regression model is $f_D(\omega) = \sum_{i=1}^{n}(y_i - x_i^T\omega)^2$, and its sensitivity without considering c is $\Delta f = 2d^2 + 4d$ in the function mechanism [15], where d represents the dimension of the attribute in the dataset. Decomposing the objective function into polynomials, we get

$$f_D(\omega) = \sum_{t_i\in D}(y_i)^2 - \sum_{j=1}^{d}\left(2\sum_{t_i\in D}y_i x_{ij}\right)\omega_j + \sum_{1\le j,l\le d}\left(\sum_{t_i\in D}x_{ij}x_{il}\right)\omega_j\omega_l$$

Then, we set

$$g_D(\omega) = \sum_{1\le j,l\le d}\left(\sum_{t_i\in D}x_{ij}x_{il}\right)\omega_j\omega_l,$$

$$h_D(\omega) = \sum_{j=1}^{d}\left(2\sum_{t_i\in D}y_i x_{ij}\right)\omega_j$$

According to the definition of sensitivity and the above inequality, we can calculate the sensitivity of $g_D(\omega)$ and $h_D(\omega)$.

$$\begin{aligned}\Delta f_1 &= \max_{D,D'} \|g_D(\omega) - g_{D'}(\omega)\|_1 \\ &\leq 2\max \sum\nolimits_{1\leq j,l\leq d} \left\|x_{ij}x_{il}\right\|_1 \leq 2d^2 \\ \Delta f_2 &= \max_{D,D'} \|h_D(\omega) - h_{D'}(\omega)\|_1 \\ &\leq 2\max(2\sum\nolimits_{j=1}^{d} yx_{(j)}) \leq 4d\end{aligned}$$

Thus, we get $\Delta f = \Delta f_1 + \Delta f_2$.

Next, we show the proof in the logistic regression model with differential privacy. In function mechanism [15], the objective function of logistic regression is approximated as a combination of polynomials by using the Taylor Formula.

$$f_D(\omega) = \sum\nolimits_{i=1}^{n} \sum\nolimits_{k=0}^{2} \frac{f_1^k(0)}{k!}(x_i^T\omega)^k - (\sum\nolimits_{i=1}^{n} y_i x_i^T)\omega$$

Its sensitivity is $\Delta f = d^2/4 + 3d$, and d represents the dimension of the attribute in the dataset. Decomposing the objective function into polynomials, we get

$$f_D(\omega)(\frac{1}{2}\sum\nolimits_{i=1}^{n} x_i^T - \sum\nolimits_{i=1}^{n} y_i x_i^T)\omega + \frac{1}{8}\sum\nolimits_{i=1}^{n} (x_i^T)^2\omega^2$$

Then, we set

$$\begin{aligned}g_D(\omega) &= \frac{1}{8}\sum\nolimits_{i=1}^{n} (x_i^T)^2\omega^2, \\ h_D(\omega) &= (\frac{1}{2}\sum\nolimits_{i=1}^{n} x_i^T - \sum\nolimits_{i=1}^{n} y_i x_i^T)\omega\end{aligned}$$

As the same, we can calculate the sensitivity of $g_D(\omega)$ and $h_D(\omega)$.

$$\begin{aligned}\Delta f_1 &= \max_{D,D'} \|g_D(\omega) - g_{D'}(\omega)\|_1 \\ &\leq 2\max(\frac{1}{8}\sum\nolimits_{1\leq j,l\leq d} x_j x_l) \leq \frac{d^2}{4} \\ \Delta f_2 &= \max_{D,D'} \|h_D(\omega) - h_{D'}(\omega)\|_1 \\ &\leq 2\max(\frac{1}{2}\sum\nolimits_{j=1}^{d} x_j + \sum\nolimits_{i=1}^{d} y_i x_i) \leq 3d\end{aligned}$$

So, we get $\Delta f = \Delta f_1 + \Delta f_2$.

Theorem 3: Differentiated privacy budget allocation satisfies ϵ-differential privacy.

Proof: In the execution of the algorithm, we need to add noise to $g_D(\omega)$, $h_D(\omega)$ separately. Assuming the process of adding noise to $g_D(\omega)$, $h_D(\omega)$ are algorithm k_1 and algorithm k_2. In function mechanism, adding noise to the monomial coefficients which include ω in the objective function satisfies the definition of differential privacy, so k_1 and k_2 satisfy ϵ_1-differential privacy and ϵ_2-differential privacy. The algorithm of differentiated privacy budget allocation is composed of k_1 and k_2, and $\epsilon_1 + \epsilon_2 = \epsilon$. According to the sequence composition characteristic of differential privacy, the algorithm of DPBA satisfies ϵ-differential privacy.

V. PERFORMANCE EVALUATION

A. EXPERIMENTAL ENVIRONMENT AND DATA

We conduct extensive experimental results on both US Census data set and Brazilian Census data set from the UCI Machine Learning Database, which contains 370057 and 188846 samples, respectively. These two data sets include 13 attributes, such as name, age, marital status, etc. Since the marital status exceeds two values, the marital status is converted into a single/married attribute, after which the transformed data set becomes 14 dimensions. We use the annual income attribute as the predicted value of the regression model. The regression task is to forecast whether the annual income of an individual is greater than 50K. For linear regression, the prediction results are numerical values. For logistic regression, the prediction results are classification (0 or 1). Before building models, the data sets need to be subjected to feature scaling to facilitate the convergence of the regression model. The experiments are executed with Intel i7 processor, 8GB RAM, 500GB hard disk, Microsoft Windows10 operating system, and the algorithms are deployed on 64-bit Matlab (2017a).

B. DIFFERENTIATED PRIVACY BUDGET ALLOCATION

The basic idea of the differentiated privacy budget allocation (DPBA) algorithm is to optimize the allocation strategy of privacy budget within the objective function. After decomposeing the objective function into polynomials, we treat each monomial term as a function, and assign different privacy budgets to different monomial term while maintaining the overall privacy budget. For regression models in this paper, the objective function is generally decomposed into a quadratic term of ω and a linear term of ω. Assuming that the privacy budget assigned to the objective function is ϵ, ϵ is assigned to the two monomial as ϵ_1 and ϵ_2, and we have $\epsilon_1 + \epsilon_2 = \epsilon$. In the first experiment, four different privacy budgets are given, which are 0.1, 1.0, 2.0, 4.0. We use 80% as training set and 20% as test set. The experiment tests the variation of the mean square error (for linear regression) or the predicition error rate (for logistic regression) under different combinations of ϵ_1 and ϵ_2. We set the privacy budget ϵ_1 assigned to quadratic term of ω as the abscissa. Fig.3 shows the fitting effect of the differential privacy budget allocation algorithm in linear regression, and Fig.4 shows the fitting effect of the differential privacy budget allocation algorithm in logistic regression.

For different data sets or different privacy budgets, both Fig.3 and Fig.4 roughly show such a tendency, with the increase of ϵ_1, the mean square error (or predictive error rate) of the test data decreases sharply at the beginning, and then the amplitude of the decrease gradually becomes stable. Finally, when ϵ_1 approaches ϵ, it rises sharply space. It shows that privacy budget allocation methods for ϵ_1 and ϵ_2 have a great influence on the fitting effect of the test data. The regression model can be optimized by finding an optimal allocation method of privacy budget.

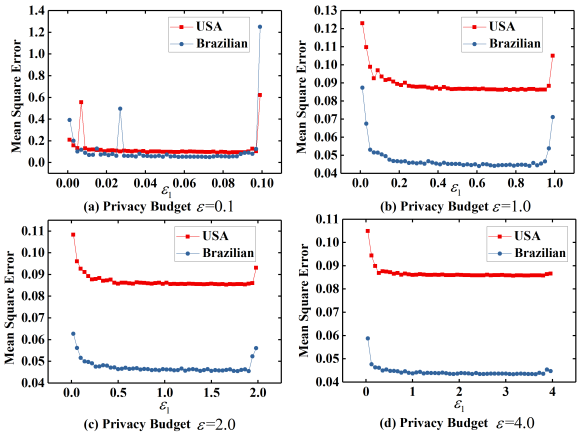


FIGURE 3. The influence of DPBA on linear regression model under different privacy budgets.

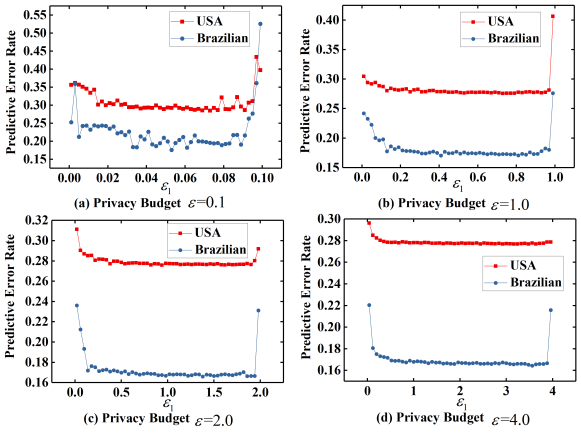


FIGURE 4. The influence of DPBA on logistic regression model under different privacy budgets.

C. MEAN SQUARE ERROR AND PREDICTION ERROR RATE

After the analysis of experiment 1, we know that the allocation method of privacy budget has a great impact of the fitting effect on the regression models. In the second experiment, we compare the proposed DPBA algorithm with four approaches, namely, FM (function mechanism) [15], DPC [18], PrivR [16] and baseline. DPC and PrivR are based on FM, which achieves differential privacy preservation in regression analysis by adding identical noise to all coefficients of the objective function in the polynomial form. DPC divides the data set into non-sensitive attributes and sensitive attributes and allocates different privacy budgets to each category. PrivR perturbs the polynomial coefficients according to the magnitude of relevance between the input features and the model output. The baseline represents the regression model without differential privacy preserving. We test six groups of privacy budgets, which were 0.1, 0.2, 0.4, 0.8, 1.6, and 3.2. All the experiments run in the data sets of US Census data and Brazilian Census data.

No matter it is linear regression shown in Fig.5 or logistic regression shown in Fig.6, DPBA is significantly improved

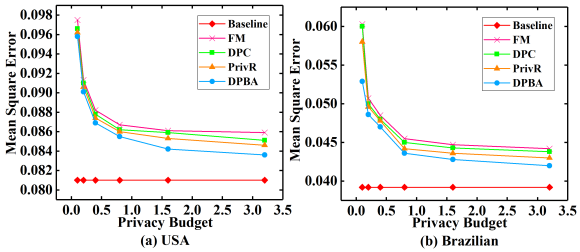


FIGURE 5. The comparison of FM, DPC, PrivR and DPBA in mean square error for linear regression.

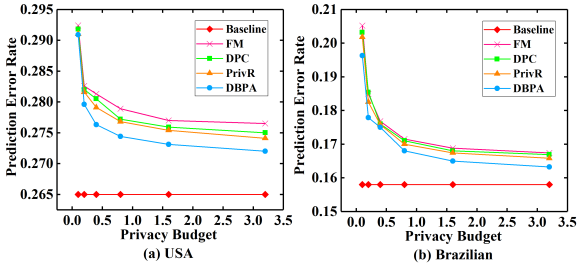


FIGURE 6. The comparison of FM, DPC, PrivR and DPBA in prediction error rate for logistic regression.

than others. And such conclusion can also be derived for different test data sets. Although, the noise has a great impact on the model, the optimization strategy of DPBA makes its fitting effect close to baseline. Function mechanism adds the same noise to each monomial term, without considering the difference between the sensitivity of monomial term. DPC and PrivR excessively consider the influence of different characteristics on the model, which makes the added noise unbalanced. However, DPBA mechanism optimizes the allocation strategy of privacy budget and minimizes the noise added to the objective function. Also, the implementation of DPBA is simpler than DPC and PrivR.

D. GENERALIZATION PERFORMANCE

The mean square error (or prediction accuracy) can only describe the regression model fitting effect partly. To more comprehensively comparing the fitting effect of DPBA and the function mechanism, it is necessary to examine the performance of the two algorithms in other aspects. In the UCI machine learning database, the census data sets are often used to test classification tasks, and the prediction result of annual income is usually divided into two categories. For the two-classification task, the generalization performance of the regression model can be evaluated by the ROC curve. In this experiment, we test the generalization performance of DPBA for logistic regression. the function mechanism is more stable than other approaches in generalization performance [16]. So, we mainly compare the generalization performance with the function mechanism. The experiment tests the generalization performance of functional mechanism and DPBA under different data sets, where privacy budgets $\epsilon = 0.1$.

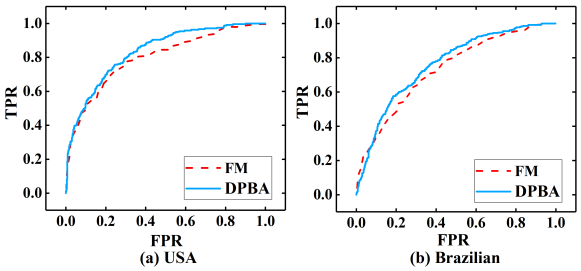


FIGURE 7. The comparison of FM and DPBA in generalization performance for logistic regression.

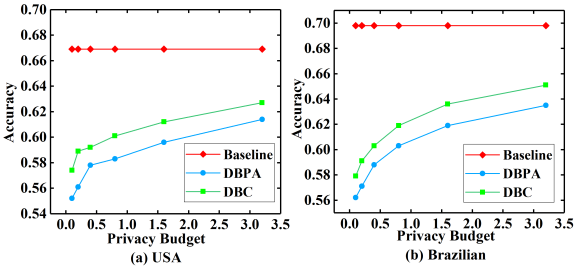


FIGURE 8. The comparison of DPC and DPBA for linear regression against model inversion attack.

Fig.7 shows that whether it is the Brazilian census data set or the US census data set, the area enclosed by ROC curve of DPBA is obviously larger than function mechanism. Therefore, the generalization performance of DPBA is better than function mechanism. In this experiment, we observe that when the selected privacy budget is small, the advantage of DPBA in generalization performance is obvious. And if the allocated privacy budget is large, the generalization performance between of the two algorithms is similar.

E. MODEL INVERSION ATTACK

The purpose of the model inversion attack is to infer an individual's sensitive attribute in the train data. In this experiment, we will test the impact of the mechanism DPBA on model inversion attack. DPC firstly proposed to defend model inversion attack in regression with differential privacy, its defense ability for model inversion attack is stronger than the function mechanism [18]. And the defense ability of PrivR is still unclear. So, we mainly compare with DPC in the experiment. We assume the adversary aims at the sensitive attribute of marital status (single/married). After the model training, we select 20% of the samples from the training set for testing. The adversary can access the model and knows values of all input attributes of the testing samples except the sensitive one. We test the defense capabilities of DPBA and DPC in six groups of privacy budgets, which were 0.1, 0.2, 0.4, 0.8, 1.6, and 3.2.

As shown in Fig.8 and Fig.9, the baseline represents the attack accuracy of the regression model without differential privacy. When the regression model has non-privacy protection, attackers can obtain sensitive information with a high degree of accuracy through model inversion attack.

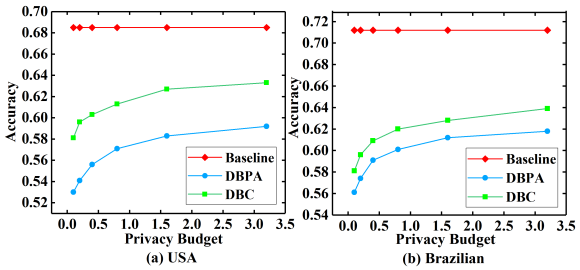


FIGURE 9. The comparison of DPC and DPBA for logistic regression against model inversion attack.

Both DPC and DPBA algorithms greatly reduce the risk of model inversion attack. Obviously, DPBA has better defense capabilities. And, as shown in experiment 2, the fitting effect of DPBA is also better than DPC. There is not much difference between the two algorithms in implementation strategy. However, DPBA is more flexible, and we can make the model have better performance by adjusting the allocation of privacy budget. Although the process of adjusting the model will increase the calculation time, the loss is worthwhile. We can get a regression model that is more suitable for the demand.

VI. SUMMARY AND FUTURE WORK

To address the problems of excessive noise and the risk of model inversion attack, which exist in the field of differential privacy regression analysis, we developed the solution named DPBA based on function mechanism and composition characteristic of differential privacy in this paper. DPBA can optimize the privacy budget allocation within the objective function while allocating privacy budgets more flexible and adjusted accordingly. Compared with the other approaches, this algorithm effectively reduces noise and achieves a balance between privacy protection and utility. On the other hand, our approach provides a new solution to prevent privacy disclosure caused by model inversion attacks. Keeping the overall privacy budget unchanged, we can modify the allocation method of internal privacy budget of an objective function to achieve different degrees of privacy protection.

In our future work, we will conduct a more in-depth study of the relationship between the distribution of privacy budgets and the size of the noise. In addition, we will find better ways to defend model inversion attacks. Furthermore, we will try to extend the DPBA mechanism to differential privacy protection of other machine learning algorithms.

REFERENCES

[1] J. O. Rawlings, S. G. Pantula, and D. A. Dickey, *Applied Regression Analysis: A Research Tool*. New York, NY, USA: Springer, 2001, pp. 1–3.
[2] B. Cai, X. Wang, P. Li, and Z. Han, "A summary of data analysis based on differential privacy," in *Proc. IEEE 4th Int. Conf. Big Data Secur. Cloud*, May 2018, pp. 79–82.
[3] X. Yang, R. Lu, K.-K. R. Choo, F. Yin, and X. Tang, "Achieving efficient and privacy-preserving cross-domain big data deduplication in cloud," *IEEE Trans. Big Data*, to be published.
[4] J. H. Abawajy, M. I. H. Ninggal, and T. Herawan, "Privacy preserving social Network data publication," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1974–1997, 3rd Quart., 2016.

[5] B. Li, Y. Liu, X. Han, and J. Zhang, "Cross-bucket generalization for information and privacy preservation," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 3, pp. 449–459, Mar. 2018.

[6] K. Mancuhan and C. Clifton, "Statistical learning theory approach for data classification with ℓ-diversity," in *Proc. SIAM Int. Conf. Data Mining*, Jun. 2017, pp. 651–659.

[7] D. Zhang, "Big data security and privacy protection," in *Proc. 8th Int. Conf. Manage. Comput. Sci.*, Atlantis, Paris, 2018.

[8] C. Dwork, "Differential privacy: A survey of results," in *Proc. Int. Conf. Theory Appl. Models Comput.* Berlin, Germany: Springer, 2008, pp. 1–19.

[9] Y. Aono, T. Hayashi, L. T. Phong, and L. Wang, "Scalable and secure logistic regression via homomorphic encryption," in *Proc. 6th ACM Conf. Data Appl. Secur. Privacy*, Mar. 2016, pp. 142–144.

[10] J. L. Raisaro, G. Choi, S. Pradervand, R. Colsenet, N. Jacquemont, N. Rosat, V. Mooser, and J.-P. Hubaux, "Protecting privacy and security of genomic data in i2b2 with homomorphic encryption and differential privacy," *IEEE/ACM Trans. Comput. Biol. Bioinformatics*, vol. 15, no. 5, pp. 1413–1426, Sep./Oct. 2018.

[11] J. H. Cheon, D. Kim, Y. Kim, and Y. Song, "Ensemble method for privacy-preserving logistic regression based on homomorphic encryption," *IEEE Access*, vol. 6, pp. 46938–46948, 2018.

[12] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, nos. 3–4, pp. 17–43, 2014.

[13] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Proc. Theory Cryptogr. Conf.* Berlin, Germany: Springer, 2006, pp. 265–284.

[14] K. Chaudhuri, C. Monteleoni, and A. D. Sarwate, "Differentially private empirical risk minimization," *J. Mach. Learn. Res.*, vol. 12, pp. 1069–1109, Mar. 2011.

[15] J. Zhang, Z. Zhang, X. Xiao, Y. Yang, and M. Winslett, "Functional mechanism: Regression analysis under differential privacy," *Proc. VLDB Endowment*, vol. 5, no. 11, pp. 1364–1375, 2012.

[16] M. Gong, K. Pan, and Y. Xie, "Differential privacy preservation in regression analysis based on relevance," *Knowl.-Based Syst.*, vol. 173, pp. 140–149, Jun. 2019.

[17] M. Fredrikson, E. Lantz, and S. Jha, "Privacy in pharmacogenetics: An end-to-end case study of personalized warfarin dosing," in *Proc. USENIX Secur. Symp.*, Aug. 2014, pp. 17–32.

[18] Y. Wang, C. Si, and X. Wu, "Regression model fitting under differential privacy and model inversion attack," in *Proc. 25th Int. Joint Conf. Artif. Intell.*, Jun. 2015, pp. 1003–1009.

[19] T. Zhu, G. Li, W. Zhou, and S. Y. Philip, "Differentially private data publishing and analysis: A survey," *IEEE Trans. Knowl. Data Eng.*, vol. 29, no. 8, pp. 1619–1638, Aug. 2017.

[20] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 308–318.

[21] N. Papernot, M. Abadi, Ú. Erlingsson, I. Goodfellow, and K. Talwar, "Semi-supervised knowledge transfer for deep learning from private training data," 2016, *arXiv:1610.05755*. [Online]. Available: https://arxiv.org/abs/1610.05755

[22] G. Li, Z. Cai, G. Yin, Z. He, and M. Siddula, "Differentially private recommendation system based on community detection in social network applications," *Secur. Commun. Netw.*, vol. 2018, Sep. 2018, Art. no. 3530123.

[23] T. T. Nguyên, X. Xiao, Y. Yang, S. C. Hui, H. Shin, and J. Shin, "Collecting and analyzing data from smart device users with local differential privacy," 2016, *arXiv:1606.05053*. [Online]. Available: https://arxiv.org/abs/1606.05053

[24] D. Kifer, A. Smith, and A. Thakurta, "Private convex empirical risk minimization and high-dimensional regression," in *Proc. Conf. Learn. Theory*, Jun. 2012, pp. 1–25.

[25] C. Dwork and V. Feldman, "Privacy-preserving prediction," 2018, *arXiv:1803.10266*. [Online]. Available: https://arxiv.org/abs/1803.10266

[26] R. Hall, A. Rinaldo, and L. Wasserman, "Differential privacy for functions and functional data," *J. Mach. Learn. Res.*, vol. 14, no. 1, pp. 703–727, 2013.

[27] X. Meng, H. Li, and J. Cui, "Different strategies for differentially private histogram publication," *J. Commun. Inf. Netw.*, vol. 2, no. 3, pp. 68–77, 2017.

[28] C. E. Rasmussen, "Gaussian processes in machine learning," in *Advanced Lectures on Machine Learning*. Berlin, Germany: Springer, 2004, pp. 63–71.

[29] M. Smith and M. Álvarez, M. Zwiessele, and N. D. Lawrence, "Differentially private regression with Gaussian processes," in *Proc. Int. Conf. Artif. Intell. Statist.*, Mar. 2018, pp. 1195–1203.

[30] M. Jagielski, A. Oprea, B. Biggio, C. Liu, C. Nita-Rotaru, and B. Li, "Manipulating machine learning: Poisoning attacks and countermeasures for regression learning," in *Proc. IEEE Symp. Secur. Privacy*, May 2018, pp. 19–35.

[31] C. Liu, B. Li, Y. Vorobeychik, and A. Oprea, "Robust linear regression against training data poisoning," in *Proc. 10th ACM Workshop Artif. Intell. Secur.*, Nov. 2017, pp. 91–102.

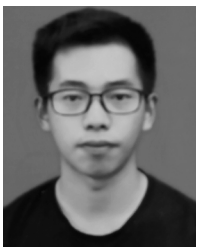
[32] M. Belkin, D. J. Hsu, and P. Mitra, "Overfitting or perfect fitting? Risk bounds for classification and regression rules that interpolate," in *Proc. Adv. Neural Inf. Process. Syst.*, 2018, pp. 2300–2311.

[33] N. Myer, J. Boland, and S. Faraone, "Pharmacogenetics predictors of methylphenidate efficacy in childhood ADHD," *Mol. Psychiatry*, vol. 23, pp. 1929–1936, Dec. 2017.

[34] B. Wang and N. Z. Gong, "Stealing hyperparameters in machine learning," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2018, pp. 36–52.

[35] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *Proc. 48th Annu. IEEE Symp. Found. Comput. Sci. (FOCS)*, Oct. 2007, pp. 94–103.

XIANJIN FANG received the Ph.D. degree in computer application technology from Anhui University, in 2010. He is currently a Professor and a M.S. Supervisor with the Anhui University of Science and Technology. His research interests include information security and data mining.



FANGCHAO YU received the B.S. degree from the Anhui University of Science and Technology, in 2018, where he is currently pursuing the master's degree. His research interests include AI security and privacy preserving.

GAOMING YANG received the master's degree in computer application from Guizhou University, in 2003, and the Ph.D. degree in computer application technology from Harbin Engineering University, in 2012. He is currently an Associate Professor and a M.S. Supervisor with the Anhui University of Science and Technology. He used to be a Visiting Scholar at the University of Arkansas for one year. His research interests include machine learning and privacy preserving.

YOUYANG QU received the B.S. and M.S. degrees from the Beijing Institute of Technology, in 2012 and 2015, respectively. He is currently pursuing the Ph.D. degree with the School of Information Technology, Deakin University. His research interests include security and privacy issues in social networks, cloud computing, the IoT, and Big Data. He has served as a TPC member for IEEE ICC 2018.