Chinese Journal of Electronics
Vol.32, No.3, May 2023

A New Edge Perturbation Mechanism for Privacy-Preserving Data Collection in IOT

CHEN Qiuling[1,2], YE Ayong[1,2], ZHANG Qiang[1,2], and HUANG Chuan[1,2]

(*1. College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350007, China*)

(*2. Fujian Provincial Key Laboratory of Network Security and Cryptology, Fuzhou 350007, China*)

Abstract — A growing amount of data containing the sensitive information of users is being collected by emerging smart connected devices to the center server in Internet of things (IoT) era, which raises serious privacy concerns for millions of users. However, existing perturbation methods are not effective because of increased disclosure risk and reduced data utility, especially for small data sets. To overcome this issue, we propose a new edge perturbation mechanism based on the concept of global sensitivity to protect the sensitive information in IoT data collection. The edge server is used to mask users' sensitive data, which can not only avoid the data leakage caused by centralized perturbation, but also achieve better data utility than local perturbation. In addition, we present a global noise generation algorithm based on edge perturbation. Each edge server utilizes the global noise generated by the center server to perturb users' sensitive data. It can minimize the disclosure risk while ensuring that the results of commonly performed statistical analyses are identical and equal for both the raw and the perturbed data. Finally, theoretical and experimental evaluations indicate that the proposed mechanism is private and accurate for small data sets.

Key words — Internet of things, Edge perturbation, Data privacy, Sensitive attribute, Statistical query.

I. Introduction

The humongous amount of data generation transforms the collection and publication of micro data [1]. It is well known that data collection [2] is the basis of Internet of things (IoT) big data applications [3]–[5]. The collected data is transferred to the cloud server and various practical applications can be achieved by analyzing the data. For example, the analysis of the collected medical data can assist medical institutions to establish mechanisms for tracking the risk of diseases in patients or help pharmaceutical companies to improve the clinical use of drugs. As a result, more and more data is being collected and analyzed in real time through sensors, wearable devices, smart sensing, video capture and other technologies. However, uploading data to cloud-based servers not only imposes significant latency and heavy communication burden, but also the data is transmitted without stricting privacy guarantees between the process and the center server. Edge computing [6] utilizes personal devices and nearby infrastructure to process data and migrates the analysis of sensitive data from cloud servers to edge servers, which can effectively reduce the risk of leakage from the center server. Therefore, the concept of edge computing based on IoT to guarantee the data usability while protecting privacy is an important research direction.

Currently, many information security and privacy protection techniques [7], [8] based on the IoT environment have been proposed. Among them, “data distortion based” techniques primarily distort sensitive data and can keep certain data or attributes unchanged [9]. Commonly used distortion methods contain randomization, swapping, blocking and enrichment, differential privacy [10], etc. There are two main perturbation mechanisms: centralized perturbation and local perturbation. The centralized perturbation is based on the premise of a trusted data collector, which is difficult to implement in practice, since we cannot guarantee that the data collector will never violate the user's data privacy or be subject to other attacks.

To solve the aforementioned problems, local perturbation has been presented to protect the privacy of users [11], [12]. It extends differential privacy to local privacy, can resist adversaries with any background knowledge, and distributes a randomization process to

Manuscript Received Nov. 23, 2021; Accepted Feb. 10, 2022. This work was supported by the National Natural Science Foundation of China (61972096, 61872090, 61771140, 61872088).

© 2023 Chinese Institute of Electronics. DOI:10.23919/cje.2021.00.411

prevent leakage from the data collector. However, each user disturbs his own data and submits it to the data collector, so none of users knows the other's data records. That means, there is no concept of global sensitivity in local perturbation, which will result in reduced protection against disclosure risk due to sampling error. Sampling error may produce different results from the analysis of perturbed data compared to the raw data, reducing data utility. In addition, local differences have both positive and negative perturbation effects on individual data, and a large number of perturbed results need to be aggregated to offset the positive and negative noise added to the data in order to obtain valid statistical results, so it cannot satisfy the needs of small data sets.

In order to overcome the problems of the above perturbation mechanisms, we develop a new edge perturbation model to protect the user's privacy information. Meanwhile, based on the existing model, a global noise generation algorithm is proposed. The main contributions of this paper are as follows:

1) We present a new edge perturbation mechanism based on the concept of global sensitivity to protect the sensitive information in IoT data collection. Unlike the centralized perturbation, the edge server is used as a suitable place to sanitize the user's sensitive data instead of uploading them to the center server. Being awareof the global sensitivity, edge perturbation can not only solve privacy issues caused by untrusted center server, but also achieve better data utility than local perturbation.

2) We also propose a global noise generation algorithm for edge perturbation. The global noise is generated by the center server through summing up local noises produced by edge servers and calculating their mean value. The sensitive data will be disturbed by the global noise, which can reduce sampling error and ensure that the results of commonly performed statistical analyses are identical and equal for both the raw and the perturbed data.

3) Experimental results demonstrate the effectiveness of the proposed scheme. The perturbed data can still maintain the same statistical properties as the raw data. In addition, the proposed scheme is compared with the local differential privacy approach, which is more effective in preserving the sensitive attributes while maintaining the data utility with uniform privacy security, and it has better adaptability to small data sets.

The rest of this paper is arranged in the following order. In Section II, we discuss the related work. Section III introduces the Preliminaries and gives the related definitions used and data utility in this paper. In Section IV, we introduce our scheme in details and present a globe perturbation algorithm. Section V presents the utility analysis and disclosure risk of our proposed edge perturbation. In Section VI, the experimental analysis is carried out. In Section VII, we conclude the paper and put forward the future research direction.

II. Related Work

1. Privacy protection methods of data

There has been a number of recent works on the privacy protection of data, which mainly include data exchange [13], [14], k-anonymity [15], [16], l-diversity [17], [18] and its improved method [19]–[21], etc. Mercedes *et al.* in [14] proposed a privacy protection method of data rank exchange, which protects data privacy from the perspective of data semantics. They sort the personal data semantically by binary relation, then divide the sorted semantic data into independent individual attributes and non-independent multiple data sets, and finally exchange the elements in the data set. Kmp *et al.* in [15] proposed a technology based on suppressing k-anonymity and multi-factor authentication. The technology includes three main processes: registration, authentication and data access. Through the suppression method, the personal identity information registered in the client is stored in the server, and then the user's identity is verified by considering multiple factors. Finally, the user can obtain the corresponding service by encrypting and decrypting the data through this technology. Mehta *et al.* in [17] proposed a scalable l-diversity privacy protection method, which is based on scalable k-anonymity to ensure that sensitive attributes in personal data records and achieve l-diversity in a certain equivalent set. Minea *et al.* in [20] proposed a comprehensive data collection scheme by using anonymous method to collect personal data. And through machine learning and specific algorithms to improve the data acquisition process. Zhou *et al.* in [21] proposed a privacy protection data collection protocol based on the improved model. Without considering the assumption of trusted third party, the data acquisition protocol ensures that the data acquisition server maximizes the data availability on the basis of k-anonymous data. However, these schemes do not provide quantitative standards for their privacy protection capabilities, and do not define the attacker's attack capability.

2. Data perturbation methods

Recently, a number of works have been reported by using perturbation methods to protect data privacy. The main idea is to add noise to desensitize the data before uploading them to the perception platform. The added noise can not only effectively protect the user's personal privacy, but also keep the statistical result unchanged. For data collection based on data perturbation, Krishnamurty *et al.* in [22] proposed firstly a data perturbation method for small data sets. Its characteristics are: the results of common statistical analysis of disturbed data are the same as those of original data. But this method has some limitations. Therefore, Tian *et al.* in [23] proposed a privacy protection mechanism, which ensures that the server does not know the identities of participants and provides relative information for the perception task. This scheme can protect the user's privacy, but the data after multiple encryption and decryption will cause huge computational overhead. In order to reduce unnecessary overhead, Wang *et al.* in [24] proposed an anonymous data collection model. The model adopts peer-to-peer network to assist anonymous data transmission and protect the sender's identity. However, the above methods can not resist background knowledge attacks and can not quantitatively analyze the privacy leakage risk of data.

Therefore, Lv *et al.* in [25] proposed a differential privacy protection method based on machine learning and maximum information coefficient. On this basis, a special privacy protection model is proposed. Firstly, the correlation sensitivity between data is accurately calculated. Then, The idea of clustering is used to realize the differential privacy protection of the whole big data association. However, the data privacy process always depends on the trusted third-party data collector, which has a certain impact on the development of differential privacy technology. Therefore, Kim *et al.* in [26] proposed a method of personal data collection based on local differential privacy, which further improves the protection of personal privacy information. The user desensitizes the data by himself, and realizes the availability of data while protecting the user's privacy. Specifically, in the case of given available targets, the method finds the optimal data disturbance scheme based on local differential privacy, which ensures the minimum total error in the disturbing process. However, the method can not maintain the relationship between data, and the errors in the process of disturbance need to be offset by a large number of positive and negative noises. For single data or small data sets, it will cause large system errors.

As we know, the above data perturbation methods can be divided into centralized perturbation and local perturbation. Centralized perturbation disturbs the collected data through the center server. Since the center server collects all data of users, it will cause a serious threat to users' privacy if the center server is attacked internally or the service provider leaks personal data for commercial interests. Furthermore, local perturbation refers to the data perturbation at the client side. However, the user's personal data set may be small, it is easy to generate a large sampling error in data perturbation processing and reduce data utility. Therefore, we develop a new edge perturbation mechanism in IoT data collection.

III. Preliminaries

1. Definitions

In general, some of the user data collected is sensitive and cannot be disclosed. For example, names, addresses, medical expenses, and disease information, etc. These are represented using sensitive attributes. And some data is not sensitive and can be disclosed. For example, gender and age, etc., which are expressed using public attributes. Therefore, assuming that the collected user data set is D, each user's data can be divided into sensitive attribute U and public attribute V. To simplify the calculation process, we assume that the dimensions of the sensitive attributes are the same as the dimensions of the public attributes in the data set, and the related definitions are as follows.

Definition 1 (The user's data set D) Supposing that the system contains m users and each user's data contains n-dimensional public attributes and n-dimensional sensitive attributes, then the user's data set $D = (U, V)$ can be defined by

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{bmatrix} \tag{1}$$

where $(a_{i1}, \dots, a_{in})$ and $(b_{i1}, \dots, b_{in})$ are the sensitive attributes and public attributes of the user i respectively.

Definition 2 (Disclosure-security) Given a data set $D = (U, V)$, $Pr(\cdot)$ is the probability of privacy disclosure. The edge perturbation mechanism M satisfies the α-disclosure-security if and only if:

$$\frac{Pr(F(V) = U)}{Pr(F(V) = U|M(U))} \le e^{\alpha} \tag{2}$$

Here, F is the prediction function; $Pr(F(V) = U)$ is the probability of predicting sensitive attributes by public attributes under the raw data; $Pr(F(V) = U|M(U))$ is the probability of predicting sensitive attributes by public attributes under the perturbation data set; α is the privacy budget, which is the level of privacy that the user ultimately enjoys; the smaller the value of α, the better the privacy. An intuitive illustration of this definition is that for any original data set and its corresponding output in M, the probability of predicting sensitive attributes by common attributes between them should be close to 1.

2. Data utility

Given the user's data set is $D=(U,V)$ and the perturbed data set is $M(D)=(Y,V)$. And A is mean value; B is standard deviation; C is covariance and D is k-order center moment. The data utility is expressed by a four tuple $T=(A,B,C,D)$:

$$T=\begin{cases} A=E_U-E_Y \\ B=S_U-S_Y \\ C=\hat{A}_{YV}-\hat{A}_{UV} \\ D=B_{kU}-B_{kY} \end{cases} \tag{3}$$

where E_U and E_Y represents the mean value of U and Y, respectively. S_U and S_Y indicates the standard deviation of U and Y, respectively. $\hat{A}_{YV}$ and $\hat{A}_{UV}$ expresss the covariance between Y and V and between U and V, respectively. B_{kU} and B_{kV} denotes the k-order center distance of U and Y, respectively. If the value of each formula in (3) is smaller, the data utility is better. Otherwise, it is worse.

3. Threat model

In our system, we assume that the edge server is trusted, which is used to disturb the raw data of users before updating them to the center server; the center server is "honest but curious," which means that it may faithfully follow our proposed protocols but try to extract as much sensitive information of users as possible. Moreover, the edge server will not collude with the center server to obtain information that they don't have access to.

IV. Proposed Scheme

1. System model

In the edge perturbation mechanism, the edge server is introduced as a perturbation node to disturb sensitive information of users before reporting to the center server, which can avoid information leakage both on users' data stored in the center server and data transmission process simultaneously. In addition, we adopt global noise to disturb the data, which can guarantee better data utility than local perturbation. The data collection model based on edge perturbation is shown in Fig.1.

In our model, users first upload raw data (RD) to their neighboring edge server, and then the edge server generates local noise (LN) using a perturbation mechanism and send it to the center server. The center server merges the local noises generated by each edge server to create global noise (GN) and returns it to each edge server. Finally, each edge server uses the global noise to disturb the user's data and reports the disturbed data (M(RD,GN)) to the center server.

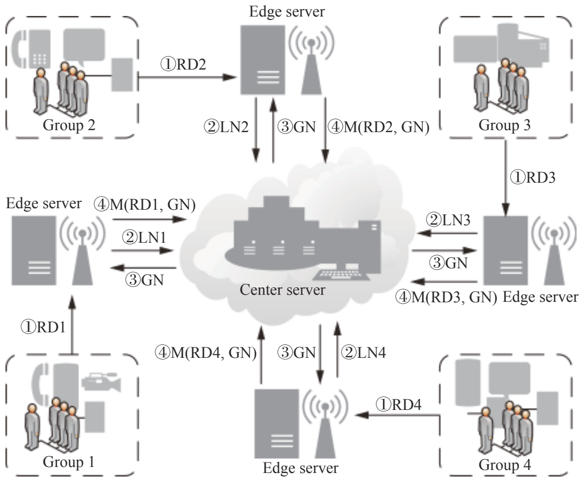

Fig. 1. Data collection model based on edge perturbation.

2. Edge perturbation mechanism

The user's data set collected by the edge server is often sparse, and there is a certain correlation between data attributes. Therefore, we present a perturbation mechanism to add noise to the raw data. The local noise is generated through the covariance between data attributes [17], and then a global noise having global sensitivity is achieved by integrating the local noise of each edge server. It can maintain the connection between data attributes and ensure the data utility. The specific perturbation process is divided into the following three steps.

1) The generation of local noise

Supposing that each group has n users, each user submits a data set (a_i,b_i), where a_i represents the sensitive variable U, b_i represents the public variable V, $(i=1,2,\dots,m)$. The local noise C is calculated by the Algorithm 1.

Step 1 The regression operation is performed on U and V, and then the regression model parameters $\hat{\beta}_0$ and $\hat{\beta}_1$ are calculated as: $\hat{\beta}_1=\frac{\hat{A}_{UV}}{\hat{A}_{VV}}$; $\hat{\beta}_0=\bar{U}-\frac{\hat{A}_{UV}}{\hat{A}_{VV}}\bar{V}$;

Step 2 The covariance $\hat{A}_{ee}=\hat{A}_{UU}-\frac{\hat{A}_{UV}}{\hat{A}_{VV}}\hat{A}_{VU}$ is calculated;

Step 3–5 The original local noise e is generated, where e obeys normal distribution $e\sim N(0,\hat{A}_{ee})$; For generated original local noise e, if $S(e)=0$, $\hat{A}_{Ue}=\hat{A}_{Ve}$, execute the next step, otherwise cycle step 3. Where $S(e)$, $\hat{A}_{Ue}$ and $\hat{A}_{Ve}$ represents respectively the standard deviation of e, the covariance matrix between U and e, V and e.

Step 6 Random matrix G is generated by standard normal distribution;

Step 7 G performs regression operation with U or V to generate the new noise H;

Step 8 The covariance $\hat{A}_{HH}$ is calculated;

Step 9 A new local noise variable C is calculated by $C=\hat{A}_{ee}^{\frac{1}{2}}\hat{A}_{HH}^{-\frac{1}{2}}$; if $S(C)=0$, $\hat{A}_{UC}=\hat{A}_{VC}$, C is local noise, otherwise cycle step 6. Where $S(C)$, $\hat{A}_{UC}$, and $\hat{A}_{VC}$ represents the standard deviation of C, the covariance matrix between U and C and between V and C, respectively.

In Algorithm 1, the noise e satisfies a normal distribution with a mean of 0. Considering the sample error, the generated actual value will be in error with the sample estimate, and the generated noise will produce some error since the noise term is independent of U and V. And the actual noise is related to U and V. Therefore, in order to satisfy the data usability, it is necessary to ensure that all n and e satisfy the following equation: $S(e) = 0$, $\hat{A}_{Ue} = \hat{A}_{Ve}$. Then, a random matrix G is generated through the standard normal distribution, and a regression of G on U or V produces a noise H and calculates its covariance matrix $\hat{A}_{HH}$. In addition, since H is orthogonal to both U and V, we have $\hat{A}_{UH} = \hat{A}_{VH}$. Let C satisfy $C = \hat{A}_{ee}^{\frac{1}{2}} \hat{A}_{HH}^{-\frac{1}{2}}$ and restrict the generated noise to satisfy $S(C) = 0$, $\hat{A}_{UC} = 0$, and $\hat{A}_{VC} = 0$, thus ensuring that the value generated by C satisfies the data utility requirement.

Algorithm 1 Local noise generation algorithm

```
Input: Original data set $D = (U, V)$;
Output: Local noise $C$;
1:  $\hat{\beta}_1 = \frac{\hat{A}_{UV}}{\hat{A}_{VV}}$;
    $\hat{\beta}_0 = \bar{U} - \frac{\hat{A}_{UV}}{\hat{A}_{VV}}\bar{V}$;
2:  $\hat{A}_{ee} = \hat{A}_{UU} - \frac{\hat{A}_{UV}}{\hat{A}_{VV}}\hat{A}_{VU}$;
3:  Do
4:  Generating perturbation noise $e$;
5:  While $S(e) \neq 0$ or $\hat{A}_{Ue} \neq \hat{A}_{Ve}$
6:  Generating random matrix $G$ by standard normal distribution;
7:  $G$ performs regression operation with $U$ or $V$ to generate new noise $H$;
8:  Calculating the covariance $\hat{A}_{HH}$ of noise $H$;
9:  Do
10: Calculating a new local noise $C$;
11: While $S(C) \neq 0$ or $\hat{A}_{UC} \neq \hat{A}_{Ve} \neq 0$
12: Return $C$.
```

2) The generation of global noise

Supposing that there are n edge servers, and the local noise is C_i, where $i = 1, 2, \dots, n$. The mean value of local noises generated by n edge servers is taken as the global noise. That is:

$$O = \frac{1}{n}\sum C_i \tag{4}$$

Then the generated global noise O is returned to each edge server.

3) Data perturbation

Edge server receives the global noise O and disturbs the raw data set. If the Y is the sensitive attribute U after perturbation, it can be expressed as:

$$Y = \hat{\beta}_0 + \hat{\beta}_1 V + O \tag{5}$$

The disturbed raw data set can be expressed as:

$$M(D) = M(U, V) = (M(U), V) = (Y, V) \tag{6}$$

where, M is the edge perturbation mechanism.

V. Theoretical Analysis

1. Data utility

The data utility of the proposed scheme is proved by comparing the statistical properties of the data before and after the perturbation. So we have the following Theorems 1 and 2.

Theorem 1 Using global noise O to disturb the data that can ensure the value of each formula in T keep 0.

Proof Assuming that the data set $D_i = (U_i, V_i)$, and the perturbed data set $M(D_i) = (Y_i, V_i)$, where $i = 1, 2, \dots, n$. The local noise C_i is produced by D_i, and the calculated parameters are $\hat{\beta}_{i0}$ and $\hat{\beta}_{i1}$, and $E(C_i) = 0$. So that the global noise is $O = \frac{1}{n}\sum C_i$.

Because:

$$\begin{aligned}
E(D_i) &= E(U_i, V_i) = E(\hat{\beta}_{i0} + \hat{\beta}_{i1}V_i) \\
&= E(\hat{\beta}_{i0}) + E(\hat{\beta}_{i1}V_i) \\
E(M(D_i)) &= E(Y_i, V_i) = E(\hat{\beta}_{i0} + \hat{\beta}_{i1}V_i + C_i) \\
&= E(\hat{\beta}_{i0}) + E(\hat{\beta}_{i1}V_i) + E(C_i) \\
&= E(\hat{\beta}_{i0}) + E(\hat{\beta}_{i1}V_i) \\
E\left(\sum_{i=1}^{n} D_i\right) &= \sum_{i=1}^{n} E(D_i) = E(D_1) + \cdots + E(D_n) \\
&= E(\hat{\beta}_{10}+\hat{\beta}_{11}V_1) + \cdots + E(\hat{\beta}_{n0}+\hat{\beta}_{n1}V_n)
\end{aligned} \tag{7}$$

$$\begin{aligned}
&E\left(\sum_{i=1}^{n} M(D_i)\right) \\
&= \sum_{i=1}^{n} E(M(D_i)) \\
&= E(M(D_1)) + \cdots + E(M(D_n)) \\
&= E(\hat{\beta}_{10} + \hat{\beta}_{11}V_1 + C_1) + \dots \\
&\quad + E(\hat{\beta}_{n0} + \hat{\beta}_{n1}V_n + C_n) \\
&= E(\hat{\beta}_{10}) + E(\hat{\beta}_{11}V_1) + E(C_1) + \cdots \\
&\quad + E(\hat{\beta}_{n0}) + E(\hat{\beta}_{n1}V_n) + E(C_n) \\
&= E(\hat{\beta}_{10}) + E(\hat{\beta}_{11}V_1) + E(\hat{\beta}_{20}) \\
&\quad + E(\hat{\beta}_{21}V_2) + \cdots + E(\hat{\beta}_{n0}) + E(\hat{\beta}_{n1}V_n) \\
&= E(D_1) + E(D_2) + \cdots + E(D_n) \\
&= \sum_{i=1}^{n} E(D_i) = E\left(\sum_{i=1}^{n} (D_i)\right)
\end{aligned} \tag{8}$$

And since $O = \frac{1}{n}\sum_{i=1}^{n} C_i$ and $E(C_i) = 0$, replace the noise C_i with O, there are:

$$E(O) = E(\frac{1}{n}\sum_{i=1}^{n} C_i) = \frac{1}{n}E(\sum_{i=1}^{n} C_i) = \frac{1}{n}\sum_{i=1}^{n} E(C_i) \quad (9)$$

Therefore, we have the following formula:

$$\begin{aligned} &E(\sum_{i=1}^{n} M(D_i)) \\ &\quad = \sum_{i=1}^{n} E(M(D_i)) \\ &\quad = E(M(D_1)) + \cdots + E(M(D_n)) \\ &\quad = E(\hat{\beta}_{10} + \hat{\beta}_{11}V_1 + O) + \cdots \\ &\quad\quad + E(\hat{\beta}_{n0} + \hat{\beta}_{n1}V_n + O) \\ &\quad = E(\hat{\beta}_{10}) + E(\hat{\beta}_{11}V_1) + E(O) + \cdots \\ &\quad\quad + E(\hat{\beta}_{n0}) + E(\hat{\beta}_{n1}V_n) + E(O) \\ &\quad = E(\hat{\beta}_{10}) + E(\hat{\beta}_{11}V_1) + E(\hat{\beta}_{20}) \\ &\quad\quad + E(\hat{\beta}_{21}V_2) + \cdots + E(\hat{\beta}_{n0}) + E(\hat{\beta}_{n1}V_n) \\ &\quad = E(D_1) + E(D_2) + \cdots + E(D_n) \\ &\quad = \sum_{i=1}^{n} E(D_i) = E(\sum_{i=1}^{n}(D_i)) \end{aligned} \quad (10)$$

It can be seen from the above theorem that the mean value (A) of data before and after perturbation remains unchanged, that is, its standard deviation (A) remains unchanged. Similarly, the covariance (C) and k-order central moment (D) of the data before and after the perturbation remain unchanged.

Therefore, the statistical analysis result of the perturbed data set $M(D) = (Y, V)$ is equal to that of the original data set $D = (U, V)$.

Theorem 2 The privacy disclosure risk of the perturbed data caused by global noise O is lower than that caused by local noise C.

Proof The disclosure risk is determined by the ratio of the intruder's ability to predict sensitive data from the public data before and after perturbing sensitive data. In this paper, we adopt a typical correlation analysis to measure the data disclosure risk. It is assumed that U is the sensitive variable, V is the public variable, and Y is the variable after data perturbation. To assess the predictive ability before perturbing the data, the public attribute is used to predict the value of sensitive variable. The correlation between U and V is ρ_1: $\rho_1 = \frac{cov(U,V)}{\sqrt{var(U)}\sqrt{var(V)}}$. To evaluate the predictive ability of the perturbed data, we also use the public variable to predict the value of sensitive variable. The correlation between Y and V is ρ_2: $\rho_2 = \frac{cov(Y,V)}{\sqrt{var(Y)}\sqrt{var(V)}}$.

In order to satisfy the data disclosure risk of (2), that is $\frac{\rho_1}{\rho_2} \le e^{\alpha}$, where $\beta_1 = \frac{A_{\hat{UV}}}{A_{\hat{VV}}}$. Because

$$\begin{aligned} cov(U,V) &= E(UV) - E(U)E(V) \\ cov(Y,V) &= E(YV) - E(Y)E(V) \\ var(U) &= E^2(U) - [E(U)]^2 \\ var(V) &= E^2(V) - [E(V)]^2 \\ var(Y) &= E^2(Y) - [E(Y)]^2 \end{aligned} \quad (11)$$

In addition, we have $Y = \hat{\beta}_0 + \hat{\beta}_1 V + e$, $E(Y) = E(U) = E[M(U)]$, where $\hat{\beta}_0$, $\hat{\beta}_1$, O are constants. Therefore,

$$\begin{aligned} var(Y) &= var(\hat{\beta}_0 + \hat{\beta}_1 V + O) \\ &= var(\hat{\beta}_1 V) + var(\hat{\beta}_0 + O) \\ &= \hat{\beta}_1^2 var(V) + var(\hat{\beta}_0) + var(O) \\ &\quad + 2E[\hat{\beta}_0 - E(\hat{\beta}_0)][E[O - E(O)] \\ &= \hat{\beta}_1^2 var(V) \end{aligned} \quad (12)$$

Because

$$\begin{aligned} & var(\hat{\beta}_0) = 0 \\ & 2E[\hat{\beta}_0 - E(\hat{\beta}_0)][E[O - E(O)] = 0 \end{aligned} \quad (13)$$

we have $var(Y) = \hat{\beta}_1^2 var(V)$ and

$$\begin{aligned} \frac{\rho_1}{\rho_2} &= \frac{cov(U,V)}{\sqrt{var(U)}\sqrt{var(V)}} \Big/ \frac{cov(Y,V)}{\sqrt{var(Y)}\sqrt{var(V)}} \\ &= \frac{\sqrt{var(Y)}}{\sqrt{var(V)}} \\ &= \frac{\sqrt{\hat{\beta}_1^2 var(V)}}{\sqrt{var(V)}} \\ &= \hat{\beta}_1 \end{aligned} \quad (14)$$

Let the inequality $\frac{Pr(F(V)=U)}{Pr(F(V)=U|M(U))} \le e^{\alpha}$ holds, just need to $e^{\alpha} \ge \hat{\beta}_1$ be satisfied. That is, when $\alpha \ge ln\hat{\beta}_1$, the inequality holds, where $\hat{\beta}_1 = \frac{A_{\hat{UV}}}{A_{\hat{VV}}}$.

Therefore, if the correlation ratio of the data before and after perturbation is $\hat{\beta}_1$, then the value of $\hat{\beta}_1$ is related to the covariance and variance between sensitive attributes. From a global perspective, the larger the data set, the greater the difference on the data; the greater the data volatility, the greater the variance of the data set. Covariance represents the overall error of two variables. The more data sets, the smaller the overall error. Therefore, the smaller the value of $\hat{\beta}_1$, the smaller the ratio of correlation coefficient between data is. Therefore, the data disclosure risk caused by global noise O is lower than that caused by local noise C.

2. Security analysis

Centralized perturbation of sensitive information is always based on one premise: a trusted third-party data collector, i.e., the guarantee that the third-party data collector will not steal or disclose sensitive information of users. However, this is unrealistic. The data collector stores all data of users, which will cause a serious threat to users' privacy if the data collector is attacked internally or the service provider leaks users' data for commercial interests. The edge perturbation mechanism proposed in this paper can solve the problem of centralized perturbation. In our model, the raw data is already disturbed before uploading to the center server, which can avoid the privacy leakage problem. In addition, the raw data is desensitized by edge nodes, even if one of edge nodes is leaked, it is only partial data, which has no significant impact on the overall results. Therefore, compared with centralized perturbation, edge perturbation can guarantee a higher level of data privacy.

VI. Experiments

In this section, statistical results and comparative results will be carried out to verify the utility and privacy risk of the proposed privacy protection mechanism for data collection based on edge perturbation, and the results will be compared with the local differential privacy proposed in [26].

1. Experimental setup

The data used in this experiment comes from the data of medical and health care center in [22]. Among them, 500 data records are reserved, and each record retains 5 data attributes. The five attributes are: name, gender, supplementary insurance, drug purchase cost and medical cost. Among them, hidden name attribute, gender and supplementary insurance as public attribute, drug purchase cost and medical cost as sensitive attribute. We randomly divided 500 groups of data into 50 groups with 10 data in each group. The data of each group were statistically analyzed. In addition, we set the group data size to 100, 200, 300, 400 and 500, and verify the effectiveness of the proposed scheme through the sensitive attributes of medical cost and procurement cost. The algorithm is implemented by MATLAB R2016a. Considering the influence of experimental error, the experiment of each group were repeated for 5 times, and the final result was the average of 5 times.

2. Statistical results

In order to obtain the attacker's predictive ability, we need to analyze the typical correlation of the data before and after the perturbation, and predict the value of sensitive variables by using the value of public variables, as shown in Fig.2.

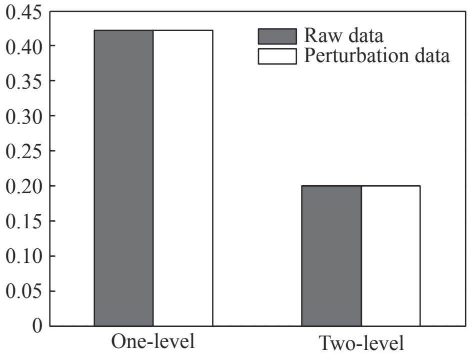

Fig. 2. Typical correlation analysis of data.

The primary and secondary correlation analysis of the original data is 0.4226 and 0.1999, respectively. For the purpose of assessing the predictive ability of the perturbed data, by repeating the above method, the primary and secondary correlations is 0.4226 and 0.1999, respectively, which is the same as the results for the original data. In other words, the predictive ability of attackers after data perturbation is the same as that raw data, and their privacy risk budget is 0.

Furthermore, the statistical queries of raw data and perturbed data are analyzed, the results are shown in Table 1 and Table 2. The names in the tables are ab-

Table 1. Marginal distribution of raw and perturbed data sets

Dataset		Marginal distribution	
		Mean value standard deviation	
Raw data	PC	504.591	81.963
	MC	1228.705	213.731
Perturbed data	PC	504.591	81.963
	MC	1228.705	213.731

Table 2. Covariance of raw and perturbed data sets

Dataset		Covariance			
		G	SI	PC	MC
Raw data	PC	−9.140	−10.49	6583.53	7201.16
	MC	−26.83	−29.55	7201.16	44767.31
Perturbed data	PC	−9.140	−10.49	6583.53	7201.16
	MC	−26.83	−29.55	7201.16	44767.31

breviations for purchase cost (PC), medical cost (MC), gender (G), and supplemental insurance (SI), respectively. As can be seen in Tables I and II, the statistical results for the mean, standard deviation and covariance are the same for both the raw and perturbed data.

3. Comparative results

The data utility of the proposed mechanism is validated and compared with the local differential privacy proposed in [26] under the same privacy level, as shown in Fig.3–Fig.9.

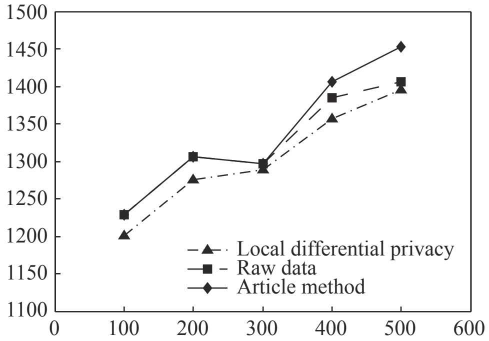

Fig. 3. Mean value of medical cost.

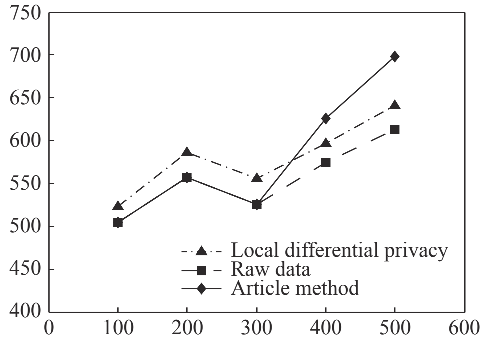

Fig. 4. Mean value of purchase cost.

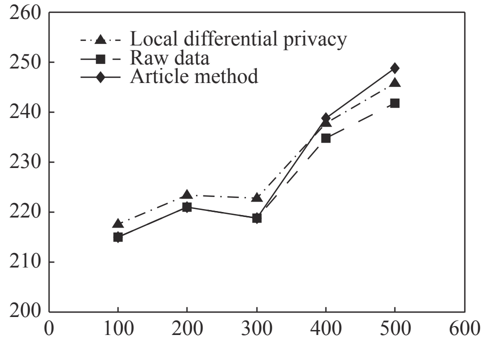

Fig. 5. Standard deviation of medical cost.

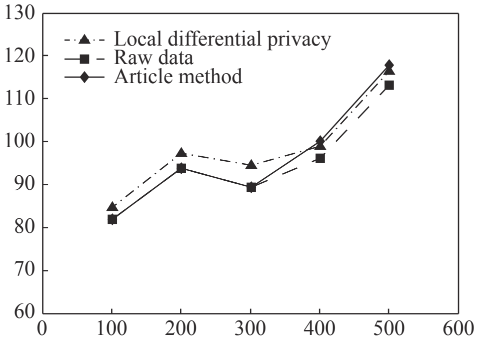

Fig. 6. Standard deviation of purchase cost.

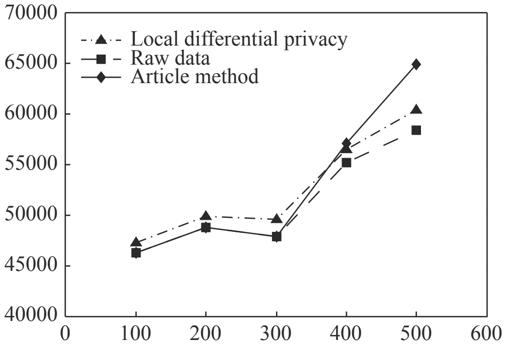

Fig. 7. 2-order central moment of medical cost.

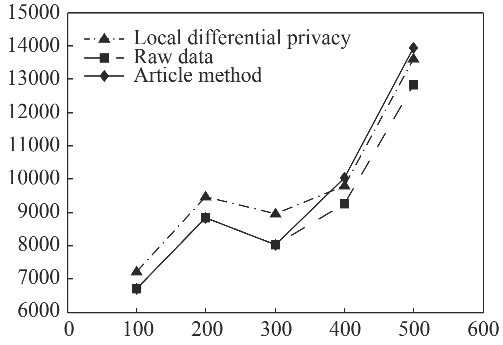

Fig. 8. 2-order central moment of purchase cost.

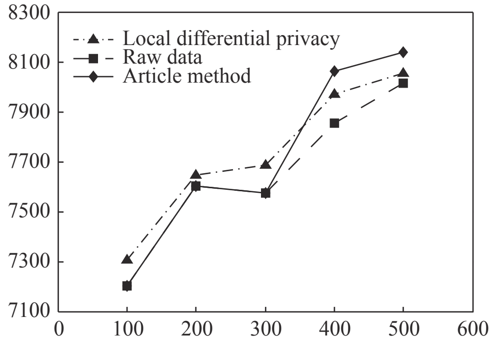

Fig. 9. Covariance of purchase cost and medical cost.

Here, the diamond point expresses the raw data, the rectangular point expresses the proposed scheme, and the triangular point expresses the local differential privacy in [26]. The abscissa represents the amount of data, and the ordinate represents the statistical results of the data. We analyze the experimental results in four aspects: mean, standard deviation, covariance, and k-order central moments.

The comparisons of mean value are shown in Fig.3 and Fig.4 . It can be seen that the mean value of the proposed method is equal to the mean value of the original data in the data set between 0 and 300, while the mean value of the data perturbed by the local differential privacy method is significantly smaller than the actual value and there is some error. However, when the data set is large, the proposed method produces larger errors. Therefore, our method is more applicable to the processing of small data sets.

It can be seen from Fig.5 and Fig.6 that local differential privacy will cause errors in each result of standard deviation and cannot truly reflect the information provided by the original data. In contrast, the proposed method can guarantee that the results of standard deviation for the perturbed data set are the same as those observed from the original data in a certain range.

Meanwhile, we analyze the k-order center distance for sensitive data of medical cost and purchase cost when $k = 2$. By calculating the distance between the original data and the disturbed data to verify the statistical results of k-order center distance, the results are shown in Fig.7 and Fig.8. It can be seen that the proposed method can guarantee that the results of 2-order central moment for the perturbed data set are the same as those observed from the original data in a certain range. For local differential privacy, the results of the 2-order central moment have some errors.

The Fig.9 shows the covariance statistics of original data, proposed method and local differential privacy. We can also find that our method has obvious advantages in a certain range.

Overall, according to the experimental results, we can see that the data utility of the proposed method is better than the local differential privacy within a certain range. That is, the proposed method can better reflect the real statistical results and provide better data utility for small data sets.

VII. Conclusions

Considering that the traditional data collection model in IoT is difficult to consider the privacy and utility of data, this paper proposes a new privacy protection mechanism based on the concept of edge perturbation. The basic idea is to introduce an edge server to protect users' sensitive data. Edge perturbation can not only avoid information leakage from the center server, but also can achieve better utility than local perturbation. In addition, we propose a global noise generation algorithm for edge perturbation. The center server collects each edge noise, merges it to generate global noise, and then sends it to each edge server. The edge servers use the global noise to perturb the data, which ensures better utility for the original data and minimizes the disclosure risk. Finally, theoretical and experimental evaluations show that the proposed mechanism has privacy and accuracy and is applicable to small data sets. In future work, we would like to consider solutions for multi-server collusion attacks. While our approach is for digital data, how to handle categorical data or convert categorical data into digital data is also a direction for future research.

References

[1] M. Abrar, B. Zuhaira, and A. Anjum, "Privacy-preserving data collection for 1: M dataset," *Multimedia Tools and Applications*, vol.80, no.20, pp.31335–31356, 2021.

[2] D. L. Lv and S. B. Zhu, "Achieving secure big data collection based on trust evaluation and true data discovery," *Computers & Security*, vol.96, article no.101937, 2020.

[3] Q. Jiang, X. Zhang, N. Zhang, *et al.*, "Three-factor authentication protocol using physical unclonable function for IoV," *Computer Communications*, vol.173, pp.45–55, 2021.

[4] G. C. Zhao, Q. Jiang, X. H. Huang, *et al.*, "Secure and usable handshake based pairing for wrist-worn smart devices on different users," *Mobile Networks and Applications*, vol.26, no.6, pp.2407–2422, 2021.

[5] Q. Jiang, N. Zhang, J. B. Ni, *et al.*, "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol.69, no.9, pp.9390–9401, 2020.

[6] B. C. M. Fung, K. Wang, R. Chen, *et al.*, "Privacy-preserving data publishing: A survey of recent developments," *ACM Computing Surveys*, vol.42, no.4, article no.14, 2010.

[7] C. Y. Wang, D. Wang, G. A. Xu, *et al.*, "Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0," *Science China Information Sciences*, vol.65, no.1, article no.11230, 2022.

[8] Z. P. Li, D. Wang, and E. Morais, "Quantum-safe round-optimal password authentication for mobile devices," *IEEE Transactions on Dependable and Secure Computing*, vol.19, no.3, pp.1885–1899, 2022.

[9] Y. X. Liu, M. S. Hu, X. J. Ma, *et al.*, "A new robust data hiding method for H. 264/AVC without intra-frame distortion drift," *Neurocomputing*, vol.151, pp.1076–1085, 2015.

[10] J. W. Kim, K. Edemacu, J. S. Kim, *et al.*, "A survey of differential privacy-based techniques and their applicability to location-based services," *Computers & Security* , vol.111, article no.102464, 2021.

[11] W. B. Fan, J. He, M. J. Guo, *et al.*, " Privacy preserving classification on local differential privacy in data centers," *Journal of Parallel and Distributed Computing*, vol.135, pp.70–82, 2020.

[12] C. Xia, J. Y. Hua, W. Tong, *et al.*, "Distributed K-means clustering guaranteeing local differential privacy," *Computers & Security*, vol.90, article no.101699, 2020.

[13] M. Nasir, A. Anjum, U. Manzoor, *et al.*, "Privacy preservation in skewed data using frequency distribution and weightage (FDW)," *Journal of Medical Imaging and Health Informatics*, vol.7, no.6, pp.1346–1357, 2017.

[14] M. Rodriguez-Garcia, M. Batet, and D. Sánchez, "Utility-preserving privacy protection of nominal data sets via semantic rank swapping," *Information Fusion*, vol.45, pp.282–295, 2019.

[15] K. Mohana Prabha and P. Vidhya Saraswathi, "Suppressed K-anonymity multi-factor authentication based Schmidt-

Samoa cryptography for privacy preserved data access in cloud computing," *Computer Communications*, vol.158, pp.85–94, 2020.

[16] S. C. Zhang, X. L. Li, M. F. Zong, *et al.*, "Learning k for KNN classification," *ACM Transactions on Intelligent Systems and Technology*, vol.8, no.3, article no.43, 2017.

[17] B. B. Mehta and U. P. Rao, "Improved l-diversity: scalable anonymization approach for privacy preserving big data publishing," *Journal of King Saud University - Computer and Information Sciences*, vol.34, no.4, pp.1423–1430, 2022.

[18] Y. W. Zhou, B. Yang, and X. Wang, "Direct anonymous authentication protocol for roaming services based on fuzzy identity," *Journal of Software*, vol.29, no.12, pp.3820–3836, 2018. (in Chinese)

[19] A. Y. Ye, J. L. Jin, Z. J. Yang, *et al.*, "Evolutionary game analysis on competition strategy choice of application providers," *Concurrency and Computation: Practice and Experience*, vol.33, no.8, article no.e5446, 2021.

[20] M. Minea and C. Dumitescu, "Enhanced public transport management employing AI and anonymous data collection," in *Proceedings of the 23rd International Conference on Circuits, Systems, Communications and Computers (CSCC 2019)*, Marathon Beach, Athens, article no.03006, 2019.

[21] Z. P. Zhou and Z. C. Li, "Data anonymous collection protocol without trusted third party," *Journal of Electronics Information Technology*, vol.41, no.6, pp.1442–1449, 2019. (in Chinese)

[22] K. Muralidhar and R. Sarathy, "An enhanced data perturbation approach for small data sets," *Decision Sciences*, vol.36, no.3, pp.513–529, 2005.

[23] Y. Tian, X. Li, A. K. Sangaiah, *et al.*, "Privacy-preserving scheme in social participatory sensing based on secure multi-party cooperation," *Computer Communications*, vol.119, pp.167–178, 2018.

[24] Y. J. Wang, Z. P. Cai, Z. Y. Chi, *et al.*, "A differentially k-anonymity-based location privacy-preserving for mobile crowdsourcing systems," *Procedia Computer Science*, vol.129, pp.28–34, 2018.

[25] D. L. Lv and S. B. Zhu, "Correlated differential privacy protection for big data," in *Proceedings of 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, Krakow, Poland, pp.1011–1018, 2018.

[26] J. W. Kim and B. Jang, "Workload-aware indoor positioning data collection via local differential privacy," *IEEE Communications Letters*, vol.23, no.8, pp.1352–1356, 2019.

CHEN Qiuling was born in 1990. She is a Ph.D. candidate of the College of Computer and Cyber Security at Fujian Normal University, Fuzhou, China. Her research interests include blockchain, network security, and location privacy.

YE Ayong (corresponding author) was born in 1977. He received the Ph.D. degree in computer system architecture from Xidian University, Xi'an, China, in 2009. He is currently a Professor and Ph.D. Supervisor of the College of Computer and Cyber Security at Fujian Normal University, China. His research interests include blockchain, network security, and location privacy. (Email: yay@fjnu.edu.cn)

ZHANG Qiang was born in 1994. He received the M.E. degree in network information security from Fujian Normal University, Fuzhou, China, in 2021. His research interests include location privacy and blockchain.

HUANG Chuan was born in 1979. He received the Ph.D. degree in communication from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2015. He is currently a Lecturer of the College of Computer and Cyber Security at Fujian Normal University, Fuzhou, China. His research interests include network attacks and information security.