A Noise Parameter Configuration Technique to Mitigate Detour Inference Attack on Differential Privacy

Taebo Jung
Dept. of Computer Engineering
Sogang University
Seoul, Korea
Inthewinter11@gmail.com

Kangsoo Jung
Dept. of Computer Engineering
Sogang University
Seoul, Korea
azure84@sogang.ac.kr

Sehwa Park
Dept. of Computer Engineering
Sogang University
Seoul, Korea
sehwapark@sogang.ac.kr

Seog Park
Dept. of Computer Engineering
Sogang University
Seoul, Korea
spark@sogang.ac.kr

***Abstract*—Nowadays, data has become more important as the core resource for the information society. However, with the development of data analysis techniques, the privacy violation such as leakage of sensitive data and personal identification exposure are also increasing. Differential privacy is the technique to satisfy the requirement that any additional information should not be disclosed except information from the database itself. It is well known for protecting the privacy from arbitrary attack. However, recent research argues that there is a several ways to infer sensitive information from data although the differential privacy is applied. One of this inference method is to use the correlation between the data. In this paper, we investigate the new privacy threats using attribute correlation which are not covered by traditional studies and propose a privacy preserving technique that configures the differential privacy's noise parameter to solve this new threat. In the experiment, we show the weaknesses of traditional differential privacy method and validate that the proposed noise parameter configuration method provide a sufficient privacy protection and maintain an accuracy of data utility.**

Keywords— privacy; differential privacy; inference attack; linear regression;

I. INTRODUCTION

Recently, personal data is explosively increased, and information that is extracted from personal data has become more important as a valuable resource for decision making. However, there is a risk that sensitive personal information can be exposed by combining with other background information. It may incur serious privacy violations. In early stages, privacy preserving technique such as de-identification, k-anonymity[1] and l-diversity are proposed to hide personal information identifiers. However, these schemes have been found that it has a vulnerability to infer sensitive information by using background knowledge such as age, gender, address, and so forth. Background knowledge may not be sensitive, but sensitive personal information can be breached through this.

Differential privacy [2, 3] is proposed to overcome the vulnerability of the anonymization technique. Differential privacy is the first successful study attempted to mathematically define the privacy protecting degree. This technique can prevent the sensitive information disclosure regardless of background knowledge[Fig. 1]. However, recent research insists that existing research on differential privacy have a weakness if there is a correlation between attributes. In this paper, we demonstrate that if the sensitive attribute has a statistical correlation with another non-sensitive attribute, the sensitive attribute's value can be inferred via the correlated non-sensitive attribute although it is protected by differential privacy. We propose a solution to protect privacy against this detour inference attack by the configuration of differential privacy's noise parameter ε appropriately.

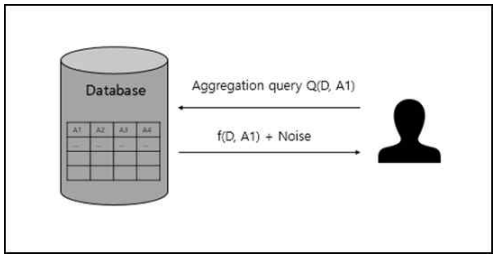

Fig. 1 Overview of the query processing using differential privacy

The rest of this paper is organized as follows. Section 2 introduces the related works on concepts and limitations of the proposed technique. Section 3 illustrates the assumptions for detour inference attack and attacker model and demonstrates some examples. Section 4 suggests a method to prevent to infer sensitive attribute value by setting an appropriate noise parameter. Section 5 verifies the proposed scheme through experiments, and Section 6 concludes the paper and discusses the future works.

II. RELATED WORKS

A. Differential Attack

The differential attack is a kind of attack to infer the value of a record by the query result difference when records insert/remove in the statistical database. Inference attack assumes the following attacker's background knowledge as follows:

- An attacker can exclude a specific record in the database as she queries the database.
- An attacker knows the query result when the specific record is excluded or not.

For example, we assume that attacker knows the number of an employee of the company A is 100 and get 30,000 dollars by querying the average annual salary of all employee of the company. After that, if an attacker gets 28,000 dollars by executing queries excluding the record of a particular employee A, an attacker may know the annual salary of A is 22,800 dollar (= 100x30,000-99x28,000). In this case, the differential attack expression is like below.

$$x = N(Avg_{before} - Avg_{after}) + Avg_{after} \quad (1)$$

B. Differential Privacys

Differential privacy is a privacy protection mechanism that prevents private information exposure that is proposed by Dwork in 2006. Dwork proposed a differential privacy to satisfy the requirement that the user should not be obtained any additional information other than the information obtained from the database itself. For this, Dwork defined a mathematical model to prevent the information exposure which ensures the privacy protection at a specified level ε, which is customized by users. Given two neighboring databases, D1 and D2, which differ by only one record, the definition of differential privacy is as follows:

Definition 1. Differential privacy[2]

A randomized function *K* provides ε-differential privacy if for all data sets D1 and D2 differing by on one element, at most and all S ⊆ Range(K), i.e.,

$$Pr[K(D1) \in S] \leq \exp(\varepsilon) \times Pr[K(D1) \in S] \quad (2)$$

Differential privacy inserts the random noise to the real output before returning the result to the user. According to the definition, the configuration of the value of ε affects the amount of added noise. As ε decreases, the privacy protection is enhanced; conversely, as ε increases, the degree of privacy protection decreases.

Definition 2. Sensitivity

$$\Delta f = \max_{(D,D')} \| f(D) - f(D') \| \quad (3)$$

The sensitivity function is the boundary of the amount of noise. It guarantees that the noise-adding mechanism covers the worst-case difference between neighboring databases.

Definition 3. Laplace mechanism

Let $f(D)$ denote a function over database D. An ε-differentially private Laplace noise mechanism is defined as $L(D) = f(D) + X$, where X is a random variable drawn from the Laplace distribution with mean = 0 and standard deviation = $\sqrt{2}\Delta f/\varepsilon$.

C. Related Works using Differential Privacy

Differential privacy becomes a *de facto* model for privacy preserving technique. It used actively in the study of various domains. We categorize previous studies as two part. The first one is an extension of differential privacy's definition and concept [4,5]. The second one is studying for applying the differential privacy concept to a specific domain [6, 7, 8]. This study belongs to former as an extension to the problem not covered by the previous differential privacy research.

Applying the differential privacy to prevent the particular person's interest location exposure when performing clustering algorithm to find the interest area [6]. [7] studies to prevent inference of particular user's information by manipulating mapper's result value when analyzing data using Hadoop map/reduce framework. [8] studies of analyzing vulnerability by correlation and improvement method of differential privacy result from applying differential privacy to graph data like social network are those of all. In particular, [8] deal with similar issues with proposed technique. However, correlation used in [8] is not as same as us because it is friend relation in the social network. Therefore it has different meaning with statistical correlation which used in this paper.

Such a previous differential privacy studies only add noise in sensitive attributes based on differential privacy. However, when inferring sensitive attribute through non-sensitive attribute which has statistically meaningful correlation with a sensitive attribute, differential privacy can be violated. In this paper define the detour inference attack and propose the appropriate noise parameter configuration technique for the non-sensitive attribute to prevent inference sensitive attribute value by correlation.

III. DETOUR INFERENCE ATTACK USING CORRELATION ATTRIBUTES

In this section, we describe the detour inference attack using non-sensitive attributes that have a correlation with sensitive attributes.

A. Applying Differential Privacy

In this paper, we assumed that the noise parameter is determined according to the sensitivity of the data when differential privacy is applied. The data sensitivity means the degree of his/her feeling about privacy violation degree when the sensitive information is exposed.

For example, Health information, such as glycemic index or blood pressure might be sensitive because this information is closely related to an individual's health condition. This sensitive data is referred as Sensitive Attribute (SA). On the other hand, there is referred as a Non-Sensitive Attribute (NSA), such as age, movie rating did not violate the individual's privacy seriously. The non-sensitive data set the

low-level privacy protection to minimize the degradation of the data utility.

B. Attacker Model

In this section, we describe the attacker model. For this, we assume that the attacker has the background knowledge that is described in Section 2.A, and can execute a regression analysis using the database information. In order to infer the SA value that is protected by the differential privacy, the attacker performs the detour inference attack using NSA which has a correlation with SA. The detour inference attack is defined as follows:

Definition 4. Detour inference attack using correlated attribute

Detour inference attack means that attack to infer the SA value approximately by using linear regression based on NSA value that has a correlation with SA.

Detour inference attack process is as follows:

First, the attacker finds the NSA that correlated with SA to infer the value of SA. If correlated NSA exists, the attacker performs a differential attack to infer the NSA's value. After then, the attacker uses the inferred NSA's value to infer the SA's value by using regression analysis. In this paper, we assume that the average query for a simple explanation. For example, height and weight data in Table. 1 have a strong correlation and its linear regression equation is as follows:

$$Height=0.9413*Weight+111.86$$

Table 1. Example Data for Detour Inference Attack

ID	Height	Weight
1	170	61
2	172	63
3	171	65
4	175	68
…	…	…
10	178	72

We assume that the height is the SA and weight is the NSA and set the noise parameter $\varepsilon = 0.1$ to SA for differential privacy, but not the NSA. In this case, when an attacker tries to infer the ID 10's height value, the average query result is a 200 because differential privacy is applied to protect privacy. Meanwhile, after obtaining a weight value 72 by the query to NSA, it is possible to infer the height value 179.6 that is similar to the real height value of ID 10 by using detour inference attack. Therefore when only differential privacy applies to SA, SA is exposed by the inference reasoning attacks although SA is protected by differential privacy.

IV. Parameter Configuration Scheme for Non-Sensitive Attribute

In this paper, we propose parameter configuration scheme for differential privacy to prevent detour inference attack. In order to maintain the performance of data utility for NSA, proposed system offers the appropriate amount of noise through the following framework.

Table 2. List of The Symbols Used in Proposed Technique

D	Database D
N	Number of Record
e_c	Correlation coefficient between attributes
e_r	Regression coefficient between attributes
b_0	y-intercept of line of regression
e_s	Safe boundary for sensitive attribute
V_{min}	Correlation boundary for non-sensitive attribute
T_{prob}	Privacy probability threshold value
Lap()	Laplace distribution function Lap()
b	Laplace distribution scaling parameter
ε	Differential noise parameter
Δf	Sensitivity
SA	Sensitive attribute
NSA	Non-sensitive attribute

A. Proposed Framework

Fig. 2 is the overall of the proposed noise parameter configuration framework.

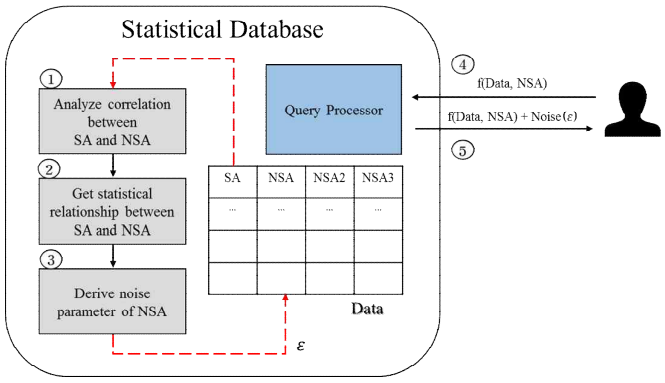

Fig. 2 Overview of the proposed noise parameter configuration technique

To prevent detour inference attack, we should find out which attributes are related to SA and determine the amount of noise for NSA. First, our framework performs a correlation analysis of sensitive and non-sensitive attribute. Then, the statistical relationship between them would be obtained by regression analysis. Using this result, it is possible to make a probabilistic model and derive the differential privacy noise parameter. Finally, when data consumer such as statistical analyst sends a query to our system, he/she will get inaccurate information which noise is added from Laplace distribution with derived parameter.

B. Privacy Rquirement

In this section, we define the privacy requirement as follows:

Definition 5. Safe Boundary(e^s)

The safe boundary is minimum error threshold when an attacker takes a detour inference attack to SA.

Domain expert set the safe boundary, and noise parameter ε should be set to keep out the inferred SA value in the safe boundary. To satisfy this requirement, we define the correlated boundary in NSA as follows:

Definition5. Correlated Boundary(V_{min})

The correlated boundary is a minimum difference of NSA value between its original value to keep the SA value's safe boundary (e^r is a regression coefficient).

$$V_{min}=e^s/e^r$$

The proposed system suggests a guideline of privacy breach area as depicted in Fig. 3. The correlated boundary makes the adversary get inaccurate query result (inference result2) while it prevents privacy violation (inference result1) for SA.

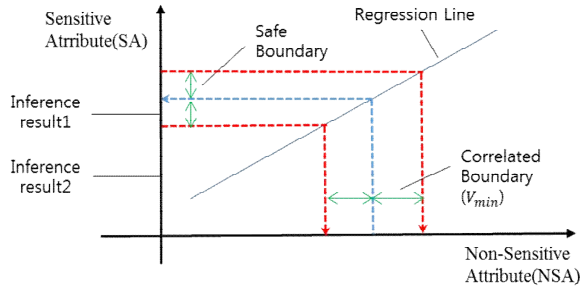

Fig. 3. Safe Boundary and Correlated Boundary

C. Linear Regression and Attribute Correlation

To solve the detour inference attack problem, we first use the Pearson correlation coefficient to calculate the correlation between SA and NSA. If a strong correlation is found, then we can calculate the statistical relationship between both attributes via linear regression analysis. By using this statistical relationship, the SA value can be inferred approximately. To prevent an inference attack, we should satisfy the differential privacy requirement of SA by injecting noise into NSA.

D. Noise Parameter Calculation

Our proposed method aims to decide the appropriate noise parameter ε for NSA (we assume the average query that is the most common statistical function). To achieve this, we calculate the noise probability distribution that satisfies both the safe boundary and the correlated boundary. To determine the noise probability distribution, we calculate the inference error that is the difference between the inferred query results and the original query results as follows:

$$Inferenceerror = N \times (Noise_D - Noise_{D'}) + Noise_D \quad (4)$$

$Noise_D$ and $Noise_{D'}$ are generated from the same Laplace distribution, and they are independent of each other.

$$\text{Laplace}(\mu = 0, b) = \frac{1}{2b} e^{-\frac{|x-\mu|}{b}} = \frac{1}{2b} e^{-\left|\frac{x}{b}\right|} \quad (5)$$

Thus, we can obtain the joint probability distribution of $Noise_D$ and $Noise_{D'}$. We set the $Noise_D$ and $Noise_{D'}$ as a random variable X and Y. The equation is as follows:

$$f_{X,Y}(x,y) = \frac{1}{2b} e^{-\frac{|x|}{b}} \bullet \frac{1}{2b} e^{-\frac{|y|}{b}} = \left(\frac{1}{2b}\right)^2 e^{-\frac{|x|+|y|}{b}} \quad (6)$$

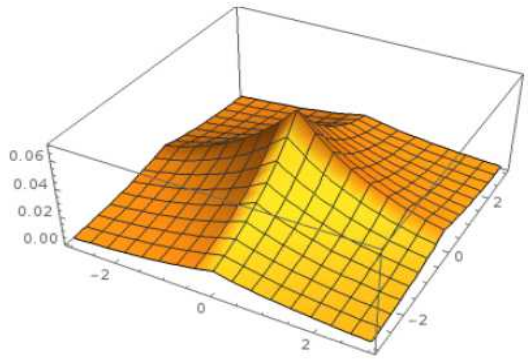

Fig. 4. Joint probability distribution

This equation's probability distribution is Fig. 4. We build the probability distribution model to estimate the amount of noise that is generated by differential privacy. By this model, we can decide the correlated boundary that does not violate the safety boundary.

$$A = \{(x,y) + y \le |V_{min}|\} \quad (7)$$

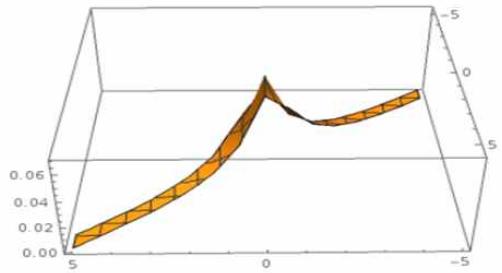

Fig. 5. Safe boundary in joint probability distribution

Summarizing the above equation with respect to y as follows:

$$y \ge \frac{N}{N-1}x - \frac{V_{min}}{N-1} \quad (8)$$

And privacy violation probability is calculated by below equation.

$$\Pr[(x,y) \in A] = \int_{-\infty}^{\infty} \int_{\frac{N}{N-1}x - \frac{V_{min}}{N-1}}^{\frac{N}{N-1}x + \frac{V_{min}}{N-1}} f_{X,Y}(x,y)dydx \quad (9)$$

The noises generated from the joint probability distribution should satisfy the correlated boundary. The following integral expression result shows the probability that satisfies the safe boundary.

$$\Pr[(x,y) \in A^c] = \int_{-\infty}^{\infty} \int_{\frac{N}{N-1}x - \frac{V_{min}}{N-1}}^{\frac{N}{N-1}x + \frac{V_{min}}{N-1}} \left(\frac{1}{2b}\right)^2 e^{-\frac{|x|+|y|}{b}} dydx \quad (10)$$

This formula can be expressed by the functional expression of b, which is the scale parameter of the Laplace distribution because the number of record N and minimum difference V_{min}

is already determined. We can obtain the value of b that satisfies the probability threshold through the functional expression, and then calculate the noise parameter ε using the following expression:

$$\varepsilon = \frac{\Delta f}{b} \quad (\ \Delta f : \text{Sensitivity of Query}) \qquad (11)$$

In the proposed technique, privacy protection level is decided by a domain expert. This privacy protection level is set by privacy probability threshold value T_{prob}. T_{prob} means that probability does not violate the safe boundary by detour inference attack. We decide the b value by T_{prob}. For example, if the domain expert set the T_{prob} as 0.9, b value is decided as below [Fig. 6].

In the proposed technique, privacy protection level is decided by a domain expert. This privacy protection level is set by privacy probability threshold value T_{prob}. T_{prob} means that probability does not violate the safe boundary by detour inference attack. We decide the b value by T_{prob}. For example, if the domain expert set the T_{prob} as 0.9, b value is decided as below [Fig. 6].

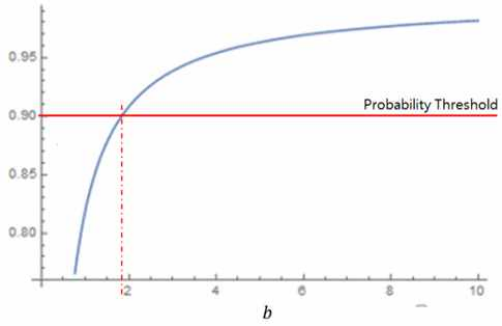

Fig. 6. Privacy Protection Probability Function

By using this noise parameter configuration technique, we can set the noise parameter which does not violate the privacy protection level and also guarantee the data utility maximization. The proposed technique's algorithm is as follows:

Algorithm1. Calculating Noise Parameter ε

INPUT:

Data set D,

Probability Threshold , T_{prob}

Correlation Threshold $T_{correlation}$

Secure variance e_s

OUTPUT:

Noise parameter ε

1. Calculate correlation coefficient C between SA and other NSAs
2. IF $C < T_{correlation}$ THEN
3. Return $\varepsilon \rightarrow \infty$
4. Calculate regression coefficient e_r
5. Calculate minimum variance V_{min}
6. Calculate Sensitivity of NSA Δf
7. Calculate probability $\Pr[(x, y) \in A]$

$$A = \{(x, y) + y \le |V_{min}|\}$$

8. Find minimum value of *b* satisfying formula

$$\Pr[(x, y) \in A] \ge T_{prob}$$

9. Calculate $\varepsilon = \frac{\Delta f}{b}$
10. Return ε

V. Experiment

In this chapter, we show that the detour inference attack and validate the proposed technique's noise parameter configuration mechanism can prevent the sensitive data exposure. We compare the proposed technique with existing differential privacy technique that does not consider correlation attributes.

A. Experimental Environment

Experiments were conducted in the environment using Windows 8.1K 64-bit, 3.30GHz Intel Core i3-3320 CPU, and 8GB memory. The experimental code was implemented in Eclipse Java EE IDE version Luna (4.4.1) in JDK 1.8.0 version of the Java language.

B. Data Set

We use the age and blood pressure data as experimental data. In general, blood pressure is medical data related to the health of the individual, so it is sensitive data. However, age is relatively less sensitive. We used the data that is provided by [11]. As we analyzed correlation for this data, the correlation coefficient was 0.84 and had a strong positive correlation. As a result of performing a regression analysis for that result, regression coefficients and regression constants were 0.9493 and 97.077, respectively. Decision coefficient was 0.7, t statistic was 8.1 and P value was 8.88E-9. Therefore, it can be said that the result of regression results was meaningful.

C. Experiment Scenario

1) Experiment settings

- The environment is assumed that quirier make a differential attack by querying age attribute which is NSA. After that, using statistical background knowledge, inference for blood pressure, which is SA, is performed.
- The situation is assumed that 100 attackers perform inference attack repeatedly 50 times each.
- The safe boundary for the SA to calculate the appropriate noise parameters in the proposed method are set to 10 and the probability threshold for privacy protection was set to be 0.90 (90%).

In the experiment, we compare proposed technique with a control group that set the noise parameters by a domain expert. The comparison is performed for a number of privacy violation, and the difference between inference value using

original data and noised data that is applied differential privacy.

We set the noise parameter by the intuition of domain knowledge for control group because existing differential privacy technique set like this. We label the noise parameter 0.01 as *strong* and noise parameter 10 as *weak*. Noise parameter value is decided by the proposed method were 0.45 and labeled it as "Proposed".

D. Experiment Analysis

At first, we show the amount of error that is generated by the differential attack to infer blood pressure attribute (SA) using age attribute (NSA). In Fig. 7, a *strong* parameter that wants to protect the privacy strongly generate a large amount of error. On the other hand, the *weak* case, it cannot satisfy the safe boundary value 10 (amount of error is 3.29).

Contrastively, the proposed technique satisfy safe boundary value 10 and also it does not make a few amount of error (amount of error is 17). It means that proposed noise parameter technique succeed to provide an appropriate noise parameter configuration that guarantee the privacy protection and also data utility.

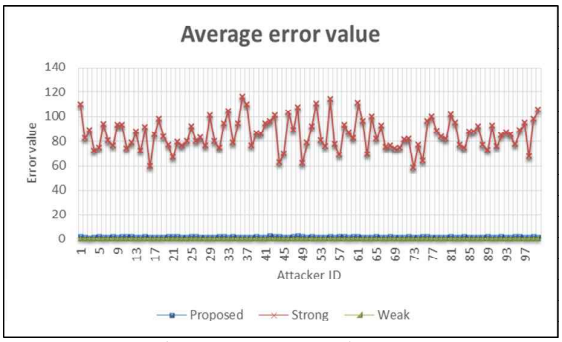

Fig. 7. Average error value

Fig. 8 show that the number of safe boundary violation. In proposed method and *strong* case, privacy violation occurs less than 10 times in 50 times of the queries averagely. However, in the case of *weak* case, the privacy might be violated by 80-90% queries.

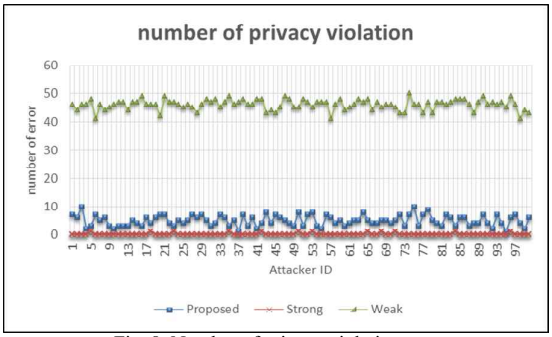

Fig. 8. Number of privacy violation

Then, we perform the experiment for the accuracy validation. Experimental results are shown in Fig. 9.

For measuring accuracy, we set the total amount of noise as a measurement value. We compare the accuracy of proposed method, *strong* and *weak* noise parameter setting. In the *strong* case, the average error value that is obtained by the average query is 109.26 in age attribute. This is a too much amount of error for age attribute. For example, if the actual average is 50 years old, those giving the almost 150 years as a return value. Next, in the case of the proposed method and *weak*, the return result is 1.7 and 0.08 that is almost same as original data. In the case of the proposed method, this result indicates the proposed can guarantee to satisfy differential privacy's requirement while it can maintain the data utility.

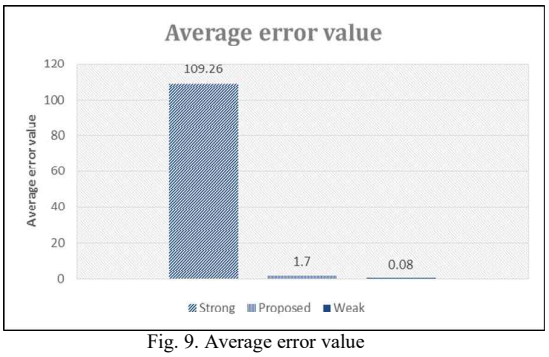

Fig. 9. Average error value

The experimental results show that proposed technique can overcome the existing differential privacy vulnerability such as detour inference attack while it does not degrade the data utility excessively.

VI. CONCLUSION

In this paper, we demonstrate that the detour inference attack which cannot be prevented by existing differential privacy techniques. The detour inference attack uses linear regression based on non-sensitive attribute value which has a correlation with a sensitive attribute that the differential privacy is applied to infer the sensitive attribute value. We define the safe boundary and correlated boundary and propose the noise parameter configuration technique to guarantee the privacy protection against detour inference attack. We validate that the proposed technique can provide a sufficient privacy protection and also does not degrade the data utility excessively. In the future work, we explore the vulnerability of the differential privacy by applying the various statistical technique to supplement the differential privacy.

ACKNOWLEDGMENT

This research was supported in part by Global Research Laboratory Program (2013K1A1A2A02078326) through NRF, DGIST Research and Development Program (CPS Global Center) funded by the Ministry of Science, ICT & Future Planning.

REFERENCES

[1] El Emam, Khaled, and Fida Kamal Dankar. "Protecting privacy using k-anonymity." Journal of the American Medical Informatics Association 15.5 pp. 627-637. 2008
[2] Dwork, Cynthia. "Differential privacy", Automata, languages and programming, p. 1, 2006.
[3] Dwork, Cynthia, et al. "Calibrating noise to sensitivity in private data analysis." Theory of cryptography, p.265, 2006.
[4] Cormode, Graham, et al. "Differentially private spatial decompositions", In IEEE 28th International Conference on Data Engineering (ICDE), p. 20, 2012.
[5] Hsu, John, et al. "Differential privacy: An economic method for choosing epsilon." Computer Security Foundations Symposium (CSF), 2014 IEEE 27th. IEEE, 2014.
[6] Ho, Shen-Shyang and Shuhua, Ruan. "Differential privacy for location pattern mining", In Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS, p. 17, 2011.
[7] Roy, Indrajit, et al. "Airavat: Security and Privacy for MapReduce", USENIX Symposium on Networked Systems Design & Implementation, p. 297, 2010.
[8] Chen, Rui, et al. "Correlated network data publication via differential privacy", The International Journal on Very Large Data Bases, 23(4), p.653, 2014.