International Journal of Control and Automation
Vol. 13, No. 2, (2020), pp. 813 – 826

Performance Analysis of Various Differential Privacy Preserving Data Distortion Techniques using Privacy Class Utility Metric

K. Sandhya Rani Kundra[1], Dr.J Hyma[2], Prof.P.V.G.D.Prasad Reddy[3],Prof.K.Venkata Rao[4]

[1] *Asst.Professor,Dept of I.T, G.V.P.Collage of Engg(A),Visakhapatnam*
[2] *Associate Professor, Dept of CSE, ANITS Engg.college(A), Visakhapatnam*
[3] *Sr.Professor, Dept of CS&SE, Andhra University, Visakhapatnam.*
[4] *Professor, Dept of CS&SE, Andhra University, Visakhapatnam.*

[1]*Email:sandhyaranikks38@gmail.com*, [2]*Email:jhyma.cse@anits.edu.in,*
[3]*Email:prasadreddy.vizag@gmail.com*, [4]*Email:professorvenkat@yahoo.com*

Abstract

Statistical database security focuses on the protection of confidential individual data, stored in databases for statistical purposes. One of the techniques used for preserving statistical database privacy is noise addition. In this technique, in response to the queries, the statistical data provided as answers are only approximate rather than exact. In this background analysis of various techniques with heterogeneous data distortion is presented in this paper. An attempt is made, to study the effect of application of various statistical measures on the distorted data, and their impact on ensuring the privacy of the original data. Experimental results show that the proposed solution outperforms traditional differential privacy in terms of Statistical Metrics on a group of queries. The performance of heterogeneous data distortion is evaluated with three types of techniques namely homogeneous with differential privacy, heterogeneous with differential privacy and also sigmoid technique (Learning model) with differential privacy. It is observed that the sigmoid technique can successfully retain the utility of published data while preserving privacy.

Keywords: *Differential Privacy, Heterogeneous, Sigmoid technique*

1. Introduction

Statistical database security is concerned with protecting privacy of individuals whose conditional data is collected through surveys or other means. In this context *individuals* can refer to person's households, companies or other entities. With the digitization being encompassing all walks of life, there is accumulation of enormous data on a daily basis. This massive collection of data and its likely sharing has added to the already growing public concern about its misuse and breach of privacy.

Privacy Preserving Data Mining (PPDM) is a prominent area concerned about the data disclosure. Its primary task in data mining is to develop models about aggregate data without letting access to original data records [1] [2]. Several privacy preserving techniques have been proposed and used in various applications. Mostly these methods followed a homogeneous data distortion technique in privacy preservation in data utility. In real time, it is not adequate because, the level of compromise in privacy is an individual choice of data disclosure and changes among datasets.

Recently Dinur and Nissim[3] and Dwork and Nissim [4] tried to provide a rigorous mathematical treatment for protecting the privacy of individuals while attempting any statistical analysis. Based on the work of Dwork et. al.[5] our research has yielded a robust privacy guarantee of *differential privacy,* which guarantees that the outcome of analysis adjacent databases that differ only in one participants information is very similar. In particular, differential privacy guarantees that participation in the analysis does not incur significant additional risk for individuals.

ISSN: 2005-4297 IJCA

A central question in this line of research regards the tradeoff between utility and privacy. In an interactive setting the queries are specified in a sharing and adaptive manner. Here the challenge lies in answering large number of queries accurately without compromising on privacy. In a recent work, Roth and Roughgarder [6] presented a new mechanism for answering queries. This efficient implementation guarantees privacy for all input databases and also gives accurate results.

To address this issue, a study is carried out on various heterogeneous data distortion techniques in data preservation and utility and reported in the present communication.

2. Related work

The problem of protecting individual privacy in the process of data collection, querying, mining and release has been researched extensively. Mainly there are two scenarios in the data privacy protection. One is the privacy preserving data publishing scenario, in which a trusted server releases datasets of individual information or answer queries on such data sets. The second one is the data collection scenario, in which an untrusted server collects personal information from different sources.

A large number of privacy preserving publishing models based on anonymity techniques such as k-anonymity [7][8], L-diversity[9] and t-closeness[10] have been proposed. Some other reports showed the implementation of privacy preserving data clustering by data transformation [11] [12]. In the perturbation approach the data is modified by the inclusion of noise component [13] [14]. Random data perturbation technique along with the necessary theoretical foundation is proposed by Kargupta et.al. [14]. they applied perturbation technique to many experimental results and observed that in most of the cases random data distortion technique failed to preserve data privacy.

The Exiting perturbation techniques follow one–size-fits-all approach which is relatively inflexible. To enhance the scope of exiting perturbation methods, Lu et.al.[15] have performed the perturbation at two different levels with different intervals. Our group attempted to study on methods to achieve maximum utility while protecting privacy in the data publishing scenario by noise-addition technique. In our analysis, we adopt the rigorous differential privacy introduced by Dwork et.al [16] that has been widely studied in the data publishing or statistical query answering scenario. The work of Lu et.al.[15] Have motivated us to perturb the data values in a heterogeneous manner. In this approach the quality of data distortion is measured in terms of various utility and privacy measures [17][18].

An empirical evaluation on amazon dataset is conducted and the performance of the different proposed techniques using differential privacy (Inverse Laplace mechanism) on heterogeneous data are compared and their statistical measures are reported. One advantage of the use of the randomized response in the data collection scenario is that the collected data can be released freely for analysis without worrying too much about privacy disclosure. This is different from the output perturbation where each additional analysis consumes further privacy budget. Moreover, the use of the randomized response for collecting data incurs less utility loss, than the output perturbation when the sensitivity of functions is high. This was demonstrated in the present study during the application of different techniques on heterogeneous data while trying to preserve differential privacy.

ISSN: 2005-4297 IJCA

International Journal of Control and Automation
Vol. 13, No. 2, (2020), pp. 813 – 826

3. Proposed technique

As single level privacy approach is not advisable for a better privacy protection and data utility, a new heterogeneous data distortion technique is reported in the previous work [19]. In this data has been classified into three different classes namely High, Medium and Low. In order to perform this classification a different privacy analysis approach is proposed. Here the privacy preference of the owner, privacy decision of the data collector and exiting correlations are taken into consideration. Using these validations, the data could be mapped to any of the convenient classes. Then accordingly perturbation with various threshold levels is introduced for different privacy classes [19] using ε-Differential privacy technique.

The stepwise details of the proposed work are presented in the following flow chart.

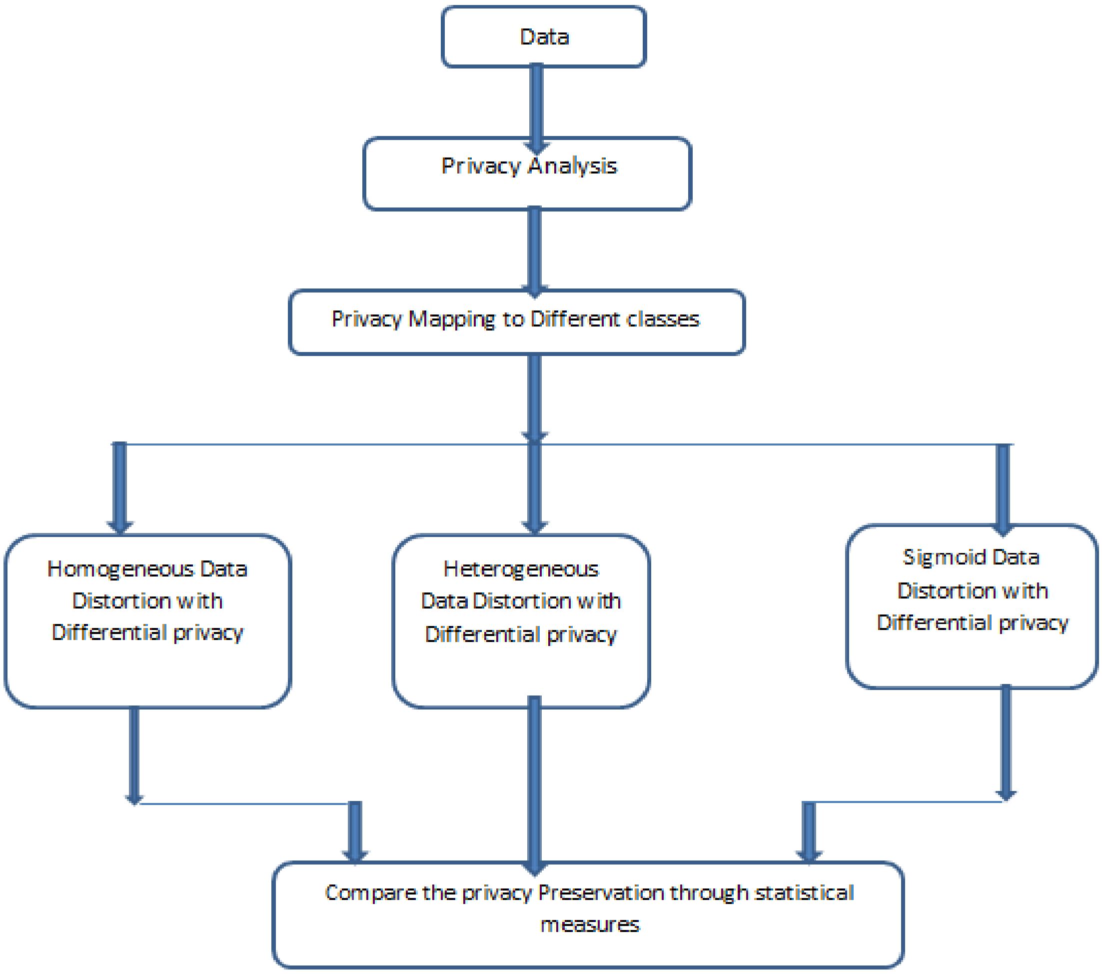

Figure 1: Flow Chart of the Proposed Work

In this approach, first data mapping is to be done into different privacy classes and then specific data distortion is performed to each of these classes. In the earlier work the performance of heterogeneous data distortion with differential privacy - three query model [19] and sigmoid learning model [20] is discussed. In sigmoid model it is demonstrated how learning models can be applied to analyze the data sensitivity and classify them into various privacy classes. Once the privacy class distribution is done the model applies Inverse Laplacian query model to check the data utility without compromising on privacy. Basing on this background the given experimental study succeeded in training the network to perform privacy analysis under a modest privacy budget, complexity training efficiency and data utility. Here it has to be ensured that the distorted data preserves its essential properties to prove its effectiveness in data utility while ensuring privacy protection with an acceptable deviation. In order to do this, the outcome of various statistical measures performed on transformed data against original data is evaluated.

3.1 Differential Privacy

This technique works by adding aptly chosen random noise to the original data to generate an answer to a query while taking care that the added noise does not deviate the answer too much from the original. In the work published earlier [21] on Differential Privacy it has been stated to enact ε-Differential Privacy by adding a random noise whose magnitude is chosen on the basis of query posed. The amount of noise added depends on the optimum change a single entity can withstand to give a meaningful and useful result.

Definition :- $f : D \rightarrow Rd$,

The L1-sensitivity of f is-

$\Delta f = \max_{D1,D2} \| f(D1) - f(D2) \|$

For all D1, D2 differing in at most one element.

Here, Δf is the sensitivity of the function f.

There are divergent noise adding mechanisms such as Laplacian, exponential, and posterior sampling used to achieve differential privacy. Laplacian and Inverse-Laplacian methods are proven to be useful in adding controlled noise to the dataset [5][22]. Here, the proposed model deals with the use of Inverse-Laplacian Mechanism to achieve differential privacy.

3.2 Inverse Laplacian Noise

The Inverse-Laplace mechanism adds a noise from the Inverse-Laplace distribution [23], which can be expressed as in Eq. 1.

$$\text{noise}(y) \propto \exp\left(-|y|/\lambda\right) \ldots\ldots \quad \text{Eq. 1}$$

which has a mean of zero and standard deviation λ. Now in this case the output function of A [23] is defined as a real valued function called as the transcript output, T_A by A and is given in Eq. 2.

$$T_A(x) = f(x) + Y \ldots. \quad \text{Eq.2}$$

where $Y \sim Lap^{-1}(\lambda)$ and f is the original real valued query or function that is planned to execute on the database. Now clearly $T_A(x)$ can be considered to be a continuous random variable [23] given in Eqs. 3 and 4 [22].

$$\frac{pdf(T_{A,D1}(x)=t)}{pdf(T_{A,D2}(x)=t)} = \frac{noise(t-f(D1))}{noise(t-f(D2))} \ldots\ldots\ldots\ldots\text{Eq. 3} \quad [23]$$

$$Lap^{-1}(u, m, b_x) = m - b_x S * sgn(u) * \ln(|1 - 2 * (u)| \ldots\ldots\ldots \text{Eq. 4}$$

$\frac{\Delta(f)}{\lambda}$ being the privacy factor ϵ which is at the most $e^{\frac{|f(D1)-f(D2)|}{\lambda}} \leq e^{\frac{\Delta(f)}{\lambda}}$ [24]. Thus T follows a differentially private mechanism (as can be seen from the definition above). It is a derived fact that in order to have A as the ϵ - differential private algorithm [23] we need to have $\lambda = \frac{1}{\epsilon}$.

Final Value

$$T_A(x) = \text{Original value}\big(f(x)\big) + \text{Lap}^{-1}(u, m, b_x)$$

Where
Lap^{-1} = Inverse Laplacian Distribution,
u = Uniform (0,1),
m = Mean,
b_x = Scaling Parameter $\frac{\Delta(f)}{\epsilon}$,
Δf is global sensitivity and ϵ is the privacy budget.

3.3 Heterogeneous Differential privacy

One of the major drawbacks of Homogeneous Noise addition is that it adds a fixed noise to each and every data set. Here, even if one of the entries is known, the noise can be calculated easily by the adversary during data extraction. This leads to violation of privacy which defeats our prime interest. Another method to add noise is using random noise addition. But sometimes an unacceptable level of noise generation results during random noise addition.

The work on Heterogeneous Differential Privacy discussed in [24], acknowledges the fact that Privacy requirements are not homogeneous across users and among the attributes from the same user. This concept of people having varied preferences can help us create a basis for adding heterogeneous noise for the posed query.

Thus, this work proposes a model where one can divide Data-Set into groups based on their privacy requirements and adding a different chunk of noise to each sub-group. This makes it difficult to find the amount of noise added, as it isn't uniform throughout.

3.4 Sigmoid-Learning based Technique

Sigmoid functions give a better deal, while dealing with the non-linear data, by providing a continuous output between 0 and 1, as a probability range. Whereas, other neural network functions like perceptron, gives a step function as output which has a disadvantage while dealing with the non-linear data. Sigmoid function output is an S shaped curve which is smoother than the step functions in the perceptron neural network. In perceptron, for every small change the result might be a complete flip, whereas in sigmoid with its S shaped output, the transaction is smooth and for every small change the result might not change drastically.

Input:

The input to sigmoid are real numbers and the output will be in the range of 0 to 1, whereby allowing to choose options for threshold values to be classified into binary.

Step-1: Initialize the parameters w, b

Step-2: Iterate until satisfied

Compute L (w, b)

$$w(t+1) = wt - \eta\Delta wt$$

$$b(t+1) = bt - \eta\Delta bt$$

Here, w and b are initialized randomly and iterated through the data. After each iteration, the squared error is computed and depending on its value the parameters are updated in such a way that the squared error is minimized.

$L(w,b) > L(w + \eta\Delta w, b + \eta\Delta b)$

The loss function is defined as follows

$\text{Loss} = \sum i\, (Zi - \hat{Z}i)^2$

Where $\hat{Z} = \frac{1}{1+e^{-(wx+b)}}$

In sigmoid the main purpose is to update the parameters w and b so that the overall loss function of the model is reduced.

3.5 Statistical Measures

Every data modification process has to be evaluated carefully. Any drastic change may negatively affect the data utility and moderate change will not add anything to preserve privacy. Hence judicious balance of these properties needs to be ensured. The following properties shown in Table -1 are used to perform this evaluation.

Table 1: List of Measures

STATISTICAL MEASURE	EQUATION
Mean	$\mu = \frac{\Sigma x}{N}$
Standard deviation	$\sigma = \sqrt{\frac{\Sigma(X-\mu)^2}{N}}$
Signal to Noise Ratio	$\text{SNR} = \frac{\mu}{\sigma}$
Mean Square Error	$\frac{1}{N}\sum_{I=1}^{N}(\mu - X)^2$
Mean Absolute Error	$\frac{1}{N}\sum_{I=1}^{N}\lvert X-\mu\rvert$
Utility Measure	**Equation**
Information Loss	(N-O) / (U-L)

Data Utility Metric (Information Loss-IL)

A new metric is introduced to measure the Utility. The basic idea is drawn from the metric proposed earlier [25]. In the proposed work the data distortion is performed at various classes, hence a variant of existing metric is imposed to measure the information loss in each of the privacy classes.

$IL_{Class} = (N_h — X_h)/(U_h — L_h)$ ……. *Eq. - 5*

N_h—New Distorted Data X_h—Original Data

U_h—Max Value in Class h, $L_{h\text{-}}$— Min Value in class h

The extent of data distortion can be assessed on the basis of information loss metric value. If the $IL_{attribute}$ measure returns a '0' value, then it means that there is no distortion and if it is '1' it implies out of range distortion. The results are shown in Fig.2. So the administrator has to take a decision to fix this parameter to optimize data utility and minimize privacy loss. This measure hopefully helps us to provide a balancing factor between the data utility and privacy.

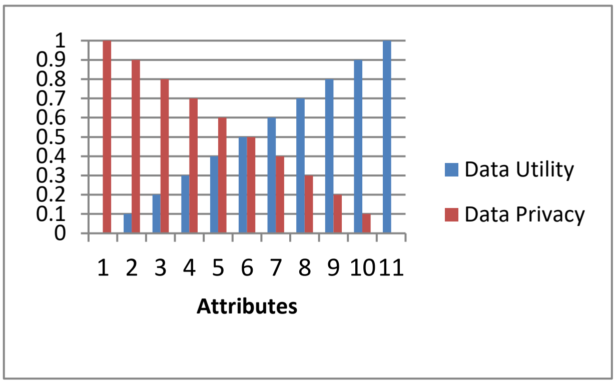

Fig. 2: Data Utility Vs Data Privacy

4. Experimental Analysis

An experiment is performed on three different data sets given in Table 2 and an illustration with sample data is shown in Table 3.

Dataset	**Attributes**	**Instances**	**Classes**
Amazon Data Set	5	2518	2
Adult Data Set	15	32561	2
Income Data set	9	18000	-

Table 2: Data Set Description

Original Data	Distorted Data using Homo-D differential Privacy	Distorted Data using Hetero-differential Privacy	Distorted Data using Sigmoid-hetero differential Privacy
15.62	16.62	17.12	18.28
15.59	17.09	17.34	18.06
15.37	15.87	16.12	16.37
15.3	16.05	16.3	16.62
15.43	15.68	16.29	16.51
15.44	15.55	15.77	16.76
15.53	17.03	17.14	18.01
15.44	15.66	16.1	16.99
15.44	15.57	15.9	16.64
15.29	15.51	15.65	16.51
15.37	15.38	17.38	18.35
15.48	15.92	18.92	19.76
15.42	16.42	16.52	16.64
15.51	16.51	16.61	16.95

Table 3: Sample Data on Amazon Data Set

Result analysis is carried out on three different transformations and finally checked with various statistical parameters. In this work we proposed a Utility metric for data modification. The administrator can check the value and accordingly can fix the threshold parameter that is privacy budget ε - value. Comparison plots for different proposed techniques are given in Figure 3 and the statistical Metric evaluation applied on Amazon data set is given in Table 4.

The Graphical representation sown in Figure 4 on three proposed transformations proved that the data pre-ordering technique showed desirable performance with respect to all statistical metrics with different deviations. The deviation rate is high in Sigmoid-Differential Privacy followed by Heterogeneous-differential Privacy followed by Homogeneous Differential Privacy. Practically, thus statically analysis is clearly shown in Figures 4 to 6.

ISSN: 2005-4297 IJCA

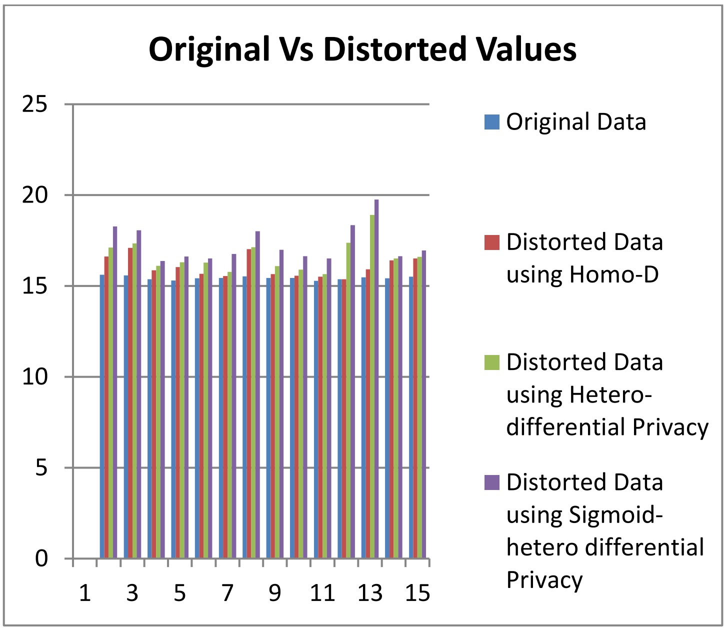

Fig. 3: Comparison of Proposed Techniques

Table 4: Metric evaluation on Amazon data set

Metrics	Original	Homo	Hetero	Sigmoid
Mean	26.51342	27.5137	28.11009	28.09897
Std Deviation	8.364222	8.371208	8.294888	8.271612
SNR	3.169861	3.286706	3.388845	3.397037
MSE	0	1.005127	2.625724	2.588186
MAE	0	1.000278	1.596668	1.585551

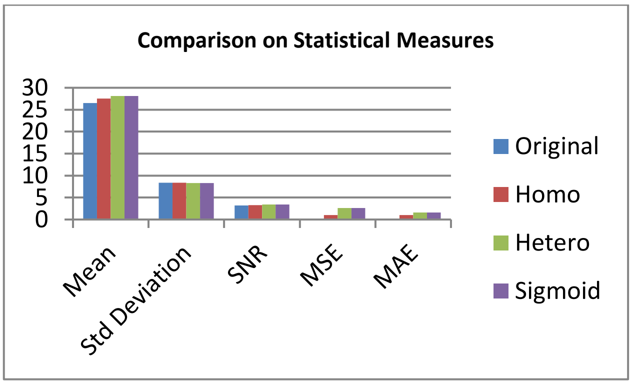

Figure 4: Comparison Plot on Statistical Measures

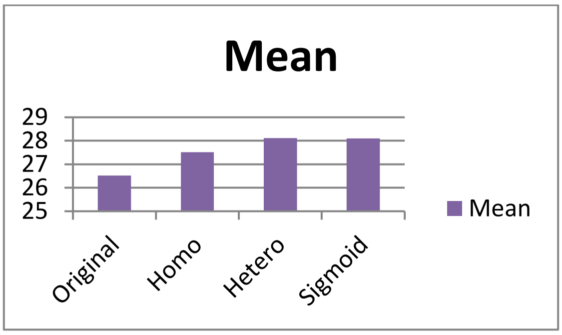

Figure 5: Comparison Plot on Mean

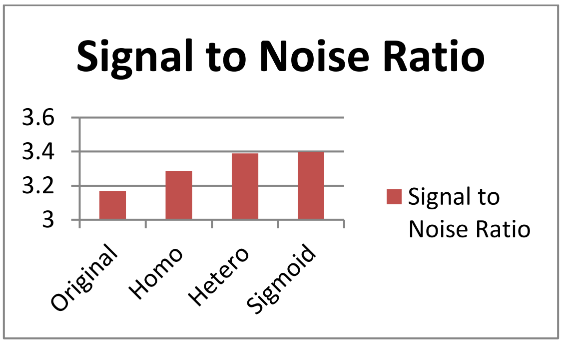

Figure 6: Comparison Plot on Signal to Noise Ratio

One more experimental statistical evaluation is conducted on different attributes by using Amazon Data Set. That is given in Table 4. Graphical representation plots for different proposed techniques are given in Figures 7 to 9.

Table 4: Metric evaluation on Attribute

Metrics	Original	Homo	Hetero	Sigmoid
Mean	112.6851	113.6878	114.3967	114.2891
Std Deviation	80.31156	80.42424	80.39715	80.57795
SNR	1.403099	1.413601	1.422896	1.418367
MSE	0	5.617072	5.61518	5.627808
MAE	0	113.6878	114.3967	114.2891

ISSN: 2005-4297 IJCA

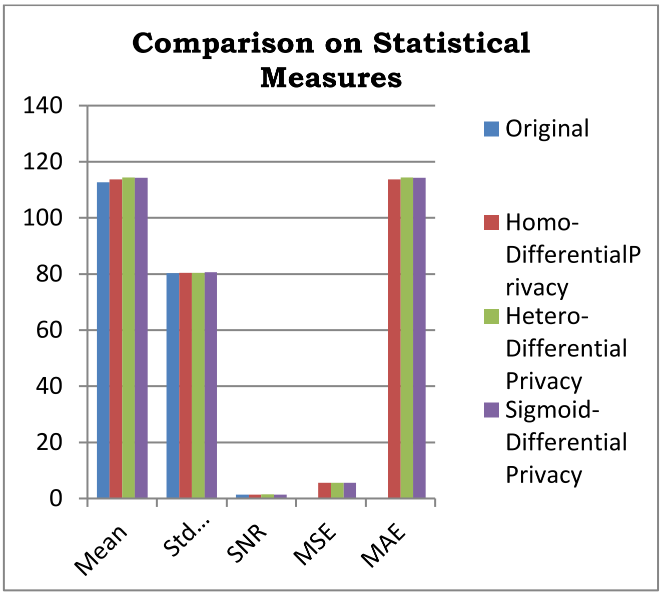

Figure 7: Comparison Plot on Statistical Measures

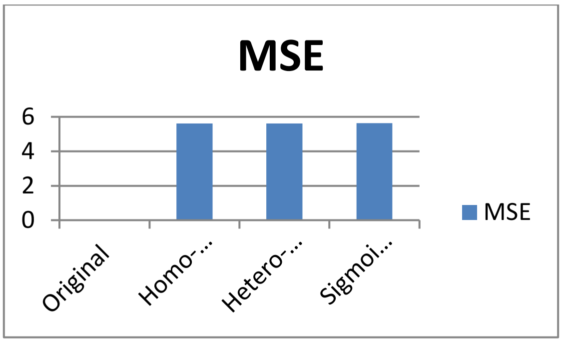

Figure 8: Comparison Plot on MSE

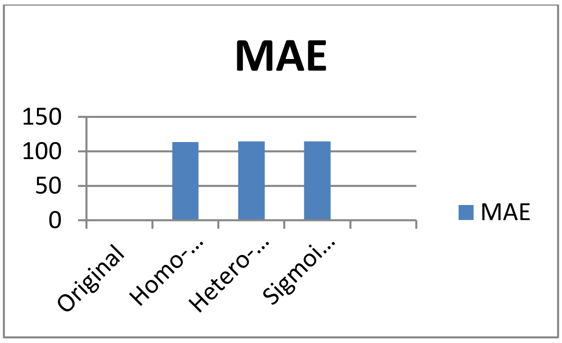

Figure 9: Comparison Plot on MAE

The information metric proposed in section 4 is applied on Amazon Data set and is evaluated for different classes of data. The closing price attribute with the Heterogeneous differential privacy has produced an IL value 0.3132 for class-1 and 0.1243 for class-2. In the attribute Daily Percent, the author has noticed an IL value of 0.5432 on class-1 and 0.3456 on class-2. The Information Loss on

ISSN: 2005-4297 IJCA

Amazon Data set with the maximum limitation as '1' representing full distortion is shown in Table 5. Graphical representation on Utility Metric is given in Figure 10.

Table 5: Data Utility on Amazon Data set

Attribute	Privacy Class	Utility Metric
Closing Price	Class1	0.3132
	Class2	0.1243
	High	1
Daily Percent Return	Class 1	0.5432
	Class 2	0.3456

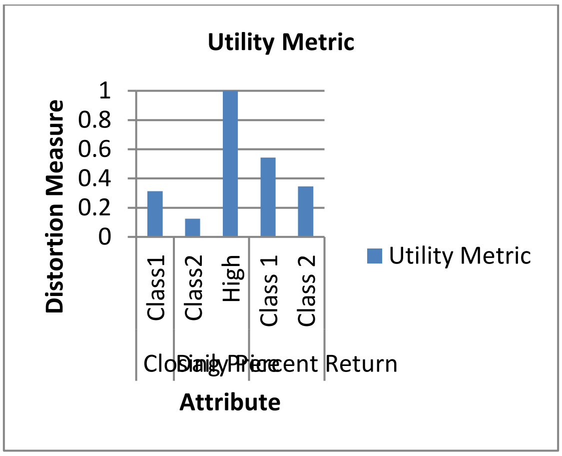

Figure 10: Graphical Representation on Utility Metric

5. Conclusion

In this paper a comparative analysis of various data transformation techniques with homogeneous and heterogeneous data distortion methods is proposed. The techniques namely homogeneous differential privacy, heterogeneous differential privacy, and sigmoid heterogeneous differential privacy have been applied to transform the data for privacy protection. These normalizations are applied at various privacy classes. The distorted data is evaluated against various distortion measures and privacy measures. A new privacy measure is implemented to measure the level of data distortion in each of the privacy class. The data analysist can take the decision on amount of noise to be added depending upon the Utility metric (IL).All the three transformation techniques are performed in accordance to the data perturbation with different data deviation rates. The present approach of data categorization into various privacy classes is adoptable to any distortion and enhances the privacy protection. The results obtained by the application of the proposed sigmoid heterogeneous differential privacy data perturbation method showed that better utility and privacy are ensured.

6. References

[1] R. Agrawal and R. Srikant. "Privacy-preserving data mining," In Proc. SIGMOD, pp. 439-450, 2000.

[2] D. Agrawal and C. Aggarwal. "On the design and quantification of privacy pre-serving data mining algorithms", In Proc. of the Twentieth ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems, Santa Barbara, California,USA, May 2001.

[3] I. Dinur and K. Nissim. “Revealing information while preserving privacy”. In Proc. 22nd PODS, pages 202–210. ACM, 2003.

[4] C. Dwork and K. Nissim. “Privacy-preserving data mining on vertically partitioned databases” , In Proc. 24thCRYPTO,pages 528–544. Springer, 2004.

[5] C. Dwork, F. McSherry, K. Nissim, and A. Smith. “Calibrating noise to sensitivity in private data analysis”. In Proc. 3rd TCC, pages 265–284. Springer, 2006.

[6] A. Roth and T. Roughgarden.,” Interactive privacy via the median mechanism”, In STOC, pages 765–774, 2010.

[7] P. Samarati and L. Sweeney, “Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression”, In Technical Report SRI-CSL-9804, SRI Computer Science Laboratory, 1998.

[8] L. Sweeney, “k-anonymity: a model for protecting privacy”, International Journal on Uncertainty, Fuzziness and Knowledgebased Systems, pp. 557-570, 2002.

[9] A.Machanavajjhala, J.Gehrke, and D.Kifer, “ℓ-diversity: Privacy beyond k-anonymity”, In Proc. of ICDE, Apr.2006.

[10] N. Li, T. Li, and S. Venkatasubramanian, “t-Closeness: Privacy Beyond k-anonymity and ℓ-Diversity”, In Proc. of ICDE, pp. 106-115, 2007.

[11] Stanley R. M. Oliveira1, Osmar R. Zaane, “Privacy Preserving Clustering by Data Transformation”, Journal of Information and Data Management”, Vol. 1, No. 1, Pages 37, February 2010.

[12] Md Zahidul Islam, Ljiljana Brankovic “Privacy preserving data mining: A noise addition framework using a novel clustering technique”, Knowledge-Based Systems, Volume 24, Issue 8, Pages 1214–1223, December 2011.

[13] Olivera, S.R.M. and Zaiane, O.R., “Privacy Preserving Clustering by Data Transformation”, Proceedings of the 18t Brazillian Symposium on Data bases, Manaus Brazil, pp.304 -318 ,2003.

[14] H. Kargupta, S.Datta, Q. Wang, K. Sivakumar, “The privacy preserving properties of random data perturbation techniques”, ICDM, IEEE Computer Society, pp. 99-106, 2003.

[15]] Li Lu, Murat Kantarcioglu, Bhavani Thuraisingham “The applicability of the perturbation based privacy preserving data mining for real-world data”, ELSEVIER, 2007.

[16] C. Dwork, F. McSherry, K. Nissim, and A. Smith. “Calibrating noise to sensitivity in private data analysis”, Theory of Cryptography, pages 265–284, 2006.

[17] Yang Xu, Tinghuai Ma, Meili Tang and Wei Tian ,” A surery of Privacy Preserving Data Publishing using Generalization and Suppression”, International Journal of Applied Mathematics& Information Sciences, 8, No. 3, 1103-1116. 2014.

[18]. Santosh Kumar Bhandare,”Data Distortion Based Privacy Preserving Method for Data Mining System”, International Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue 3, May – June 2013.

[19]. K Sandhya Rani Kundra, Dr.J.Hyma, Prof P.V.G.D Reddy, Prof.K.Venkata Rao “Privacy preserving query model using inverse laplacian differential technique”, IOP Conf. Series: Journal of Physics, 2019.

[20]. K Sandhya Rani Kundra, Dr.J.Hyma, Prof P.V.G.D Reddy, Prof.K.Venkata Rao “A Sigmoid based Learning in Heterogeneous Distortion for Data Privacy”, IJITEE, Volume-8 Issue-11, September 2019.

[21]. Cynthia Dwork and Adam Smith,”Differential Privacy for Statistics: What we Know and What we Want to Learn”, Journal of Privacy and Confidentiality. V1, pp: 135- 154, 2009.

[22] Rathindra Sarathy, Krish Muralidhar,” Differential privacy for Numeric Data “ in proceedings Joint UNECE/Eurostat work session on statistical data confidentiality ,Bilbao, Spain, 2-4 December 2009.

[23]Differential Privacy (From Wikipedia,the free encyclopedia) https://en.wikipedia.org/wiki/Differential_privacy.

[24] Mohammad Alaggan, ebastien Gambs and Anne-Marie Kermarrec “ Heterogeneous Di erential Privacy”, Journal of Privacy and Con dentiality, V7, Number 2, 127-158, 2016.

[25] Yang Xu, Tinghuai Ma, Meili Tang, Wei Tiam “A Survey of Privacy Preserving Data Publishing using Generalization and Suppression” ,Applied Mathematics & Information Sciences, 8(3):1103-1116 , May-2014.

AUTHORS PROFILE

Mrs K.SandhyaRani Kundra ,Asst.Professor in the department of Information Technology,Gayatri Vidhya Parishad College Of Engineering(A),currently perusing Ph.D. in Andhra University, Visakhapatnam. Interested areas are Privacy and security and information security.

Dr.J.Hyma,Associate Professor in the department of computer science engineering, ANITS. Her area of interest in Data Science, Internet of Things, Privacy and Security.

Prof P.V.G.D Reddy is presently Vice Chancellor, ANDHRA UNIVERSITY and Sr.Professor of Computer Science & Systems Engineering department which is the largest department in entire South India, and also serving as MEMBER, Executive Council of VIGNAN Deemed University, Guntur. He has been awarded the Best Teacher Award for the year 2011 by the Govt. of Andhra Pradesh in the combined state. Prof. Reddy's Research areas include Soft Computing, Software Architectures, knowledge Discovery from Databases, Image Processing, Number theory & Cryptosystems. He has 3 Patents granted.

Prof.K.Venkata Rao, presently Academic Dean, ANDHRA UNIVERSITY, and Professor of Computer Science & Systems Engineering department. He is currently director & chairman; teachers mutually aided cooperative society ltd. and. Honorary director and web master, Andhra University.