INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.,

Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)],

Index Copernicus Publishers Panel, Polandwith IC Value of 5.09 &number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than 2401 Cities in 155 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

Weinvite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the area of Computer, Business, Finance, Marketing, Human Resource Management, General Management, Banking, Education, Insurance, Corporate Governance and emerging paradigms in allied subjects like Accounting Education; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Monetary Policy; Portfolio & Security Analysis; Public Policy Economics; Real Estate; Regional Economics; Tax Accounting; Advertising & Promotion Management; Business Education; Management Information Systems (MIS); Business Law, Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labor Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; Public Administration; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism, Hospitality & Leisure; Transportation/Physical Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Digital Logic; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Multimedia; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic and Web Design. The above mentioned tracks are only indicative, and not exhaustive.

Anybody can submit the soft copy of his/her manuscript **anytime** in M.S. Word format after preparing the same as per our submission guidelines duly available on our website under the heading guidelines for submission, at the email address: infoijrcm@gmail.com.

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR
IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF .**

(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR:
Designation:
Affiliation with full address, contact numbers & Pin Code:
Residential address with Pin Code:
Mobile Number (s):
Landline Number (s):
E-mail Address:
Alternate E-mail Address:

NOTES:

a) The whole manuscript is required to be in ***ONE MS WORD FILE*** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
b) The sender is required to mentionthe following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/ Engineering/Mathematics/other, please specify)
c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
d) The total size of the file containing the manuscript is required to be below **500 KB**.
e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.

2. **MANUSCRIPT TITLE:** The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS:** The author (s) **full name**, **designation**, **affiliation** (s), **address**, **mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ABSTRACT:** Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.

6. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.

7. **HEADINGS:** All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

8. **SUB-HEADINGS:** All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.

9. **MAIN TEXT:** The main text should follow the following sequence:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESES

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

SCOPE FOR FURTHER RESEARCH

ACKNOWLEDGMENTS

REFERENCES

APPENDIX/ANNEXURE

It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed ***5000 WORDS***.

10. **FIGURES &TABLES:** These should be simple, crystal clear, centered, separately numbered &self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. It should be ensured that the tables/figures are referred to from the main text.

11. **EQUATIONS:**These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.

12. **REFERENCES:** The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- The location of endnotes within the text should be indicated by superscript numbers.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, KurukshetraUniversity, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

K-JOIN-ANONYMITY FOR DATABASE ON DATA PUBLISHING

S.BOOPATHY
ASST. PROFESSOR
SNS COLLEGE OF ENGINEERING
COIMBATORE

P.SUMATHI
ASST. PROFESSOR (SG)
SNS COLLEGE OF ENGINEERING
COIMBATORE

ABSTRACT

Privacy for microdata is common problem in external database and data publishing. K-anonymity is one technique to protect micro data against linkage and identification of records. While in previous k-anonymity algorithms exist for producing k-anonymous data, due to privacy issues, the common data from different sites cannot be shared directly and assumes existence of a public database that can be used to breach privacy. During anonymization process, public database are not utilized. In existing generalization algorithm creates anonymous table by using microdata table. Omission of public database leads to a high information loss. So we introduce new concept k-join-anonymity (KJA) that reduces information loss while publishing data and it is more effective generalization. KJA permits utilization of existing generalization techniques. In KJA, we adapt k-anonymity algorithm proposing two methodologies. First generalizes combination of micro data table and public database under the constraint that each group should contain at least one tuple of microdata table. In second anonymizes micro data table then refines the resulting groups using public database.

KEYWORDS
Microdata, Privacy, k-anonymity, k-join-anonymity.

1. INTRODUCTION

Many organizations are increasingly publishing microdata tables that contain unaggregated information about individuals. These tables can include medical, voter registration, census, and customer data. Microdata is a valuable source of information for the allocation of public funds, medical research, and trend analysis. However, if individuals can be uniquely identified in the microdata, then their private information (such as their medical condition) would be disclosed, and this is unacceptable. Microdata are useful for several tasks such as health research etc., Privacy for microdata aims at limiting the risk of linking published data to a particular person [1]. There are three types of microdata attributes are relevant to the privacy preservation. They are

1. Identifiers (IDs)
2. Quasi Identifiers (QIs)
3. Sensitive attributes (SAs)

IDENTIFIERS
Attributes like Name, Social Number or License Number that uniquely identify individuals
QUASI-IDENTIFIERS
Attributes like Age, Gender and Zip Code which exist in other existing external databases and may be used by combination to identify an individual that are named quasi identifier.
SENSITIVE ATTRIBUTES
Attributes like Income of Bank Customers or Disease of Hospital Patients that are important for data holder to remain private for individuals and they are named sensitive attributes.
EXAMPLE 1

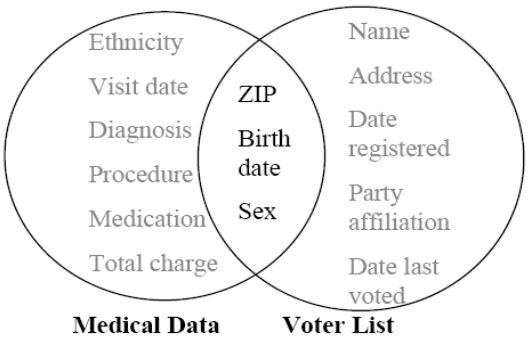
Identifier	Quasi Identifiers			Sensitive
Name	Birthdate	Gender	Zipcode	Disease
Arun	21/1/79	Male	637202	Flu
Marry	10/3/81	Female	637201	Hepatitis

Several concepts have been proposed to achieve privacy preservation. Most database literature has focused on k-anonymity [8], [10]. Specifically, a table T is k-anonymous if each record is indistinguishable from at least k-1 other tuples in T with respect to the QI set. The process of generating a k-anonymous table given the original microdata is called k-anonymization. The most common form of k-anonymization is generalization, which involves replacing specific QI values with more general ones.
The concept of K-join-anonymity permits the utilization of existing generalization techniques and protects the microdata against the linkage and identification of records during the data publishing.

2. PROBLEM DEFINITION

All the previous k-anonymity techniques are not utilizing the existence of a Public Database during the anonymization process. This omission leads to unnecessarily high information loss. Grouping the fields that contain tuples with different quasi identifiers values. Publicly available databases (voter lists, city directories) can reveal the “hidden” identity [2], [3]. Attacker can re-identify the sensitive information by using background knowledge. By using micro data table alone its create the anonymous table. Not utilizes the Public Database for generalization algorithm[5]. Sensitive attributes are not consider while data publishing. Attacker have the Background Knowledge about microdata by using public database (example: voter list, city directory). Unnecessarily high information loss.

EXAMPLE 2



In the above example attacker use the public database (voter list) to know the details of the microdata like medical data. By using background knowledge attacker know the privacy data. In the existing system there is possible for information leakage and data linking and identification problem. In this anonymous table created for microdata table alone.

To avoid the identification of records in microdata, uniquely identifying information like names and social security numbers are removed from the table. However, this first sanitization still does not ensure the privacy of individuals in the data. A recent study estimated that 87% of the population of the United States can be uniquely identified using the seemingly innocuous attributes gender, date of birth, and zip code [9]. In fact, those three attributes were used to link voter registration records (which included the name, gender, zip code, and date of birth) to supposedly anonymized medical data (which included gender, zip code, date of birth and diagnosis). This "linking attack" managed to uniquely identify the medical records of the individual [10].

2.1. ATTACKS ON *K*-ANONYMITY

In this section we present two attacks, the **homogeneity attack** and the **background knowledge attack**.

Observation 1. *k-Anonymity can create groups that leak information due to lack of diversity in the sensitive attribute.*

Observation 2. *k-Anonymity does not protect against attacks based on background knowledge.*

3. RELATED WORK

Definition 1. (Quasi-identifier)**.** *A set of nonsensitive attributes* $\{Q_1,\ldots,Q_w\}$ *of a table is called a* quasi-identifier *if these attributes can be linked with external data to uniquely identify at least one individual in the general population.*

One example of a quasi-identifier is a primary key like social security number. Another example is the set {Gender, Age, Zip Code}in the Group Insurance Company dataset that was used to identify the governor of Massachusetts as described in the introduction. Let us denote the set of all quasi-identifiers by *QI*. We are now ready to formally define *k*-anonymity.

Definition 2. *The schema of a microdata table (MT) consists of the unique ID, QI and sensitive attributes.*

Definition 3. *The schema of a public database (PD) consists of the unique ID and all QI attributes appearing in MT.*

Using PD, the attacker identifies the QI values of an individuals.

The concept of K-anonymity utilization of existing generalization techniques and protects the microdata against the linkage and identification of records during the data publishing. Anonymized table (AT) is created by using microdata table and not utilizing public database. Identifiers and sensitive information are removed and generalization is performed in the AT.

Sets of attributes (like gender, date of birth, and zip code in the example above) that can be linked with external data to uniquely identify individuals in the population are called *quasi-identifiers*. To counter linking attacks using quasi-identifiers, Samarati and Sweeney proposed a definition of privacy called *k-anonymity* [8,10] A table satisfies *k*-anonymity if every record in the table is indistinguishable from at least *k ¡*1 other records with respect to every set of quasi-identifier attributes; such a table is called a *k-anonymous* table. Hence, for every combination of values of the quasi-identifiers in the *k*-anonymous table, there are at least *k* records that share those values. This ensures that individuals cannot be uniquely identified by linking attacks.

It propose the privacy is common problem while data publishing, formerly, K-anonymity methods of Privacy Protection have great influence on the data precision[6]. This paper also analyzes the reasons of the influence, and proposes an improved algorithm. The algorithm defines a Weight-related of attribute in order to select attributes for generalization. This approach effectively prevents sensitive data loss in the generalization. Experimental results show that the improved algorithm of K-anonymity model increases the data precision effectively.

It proposes and evaluates an optimization algorithm for de-identification of data. This powerful de-identification procedure is known as *k*-anonymization[7]. A *k*-anonymized dataset has the property that each record is indistinguishable from at least *k* – 1 others. In addition, they implemented data-management strategies that avoid repeatedly sorting the entire dataset for markedly reduced node evaluation times. But it does not provide sufficient protection against attribute disclosure.

All the previous work shown the necessity of considering an attacker's background knowledge when reasoning about privacy in data publishing [3]. However, in practice, the data publisher does not know what background knowledge the attacker possesses. Thus, it is important to consider the worst-case.

In [3] this paper, they initiate a formal study of worst-case background knowledge. They propose a language that can express any background knowledge about the data. We provide a polynomial time algorithm to measure the amount of disclosure of sensitive information in the worst case, given that the attacker has at most k pieces of information in this language. We also provide a method to efficiently sanitize the data so that the amount of disclosure in the worst case is less than a specified threshold.

4. K-JOIN-ANONYMITY

K-join-anonymity permits the utilization of existing generalization techniques and protects the micro data against the linkage and identification of records during the data publishing. Join table is created by using both micro data table and public database. Identifiers and sensitive information are removed from the join table. Reduce the loss of information and provide privacy for micro data by utilizing the public database. The goal of k-join-anonymity is to provide the same privacy guarantees with k-anonymity incurring, however, less information loss. To achieve this, it shrinks the G-boxes using public knowledge about universe (U) tuples. In some applications, the entire U is available to the publisher, e.g., as in the company payroll example. First generalizes the combination of microdata table and public database under the constraint that each group should contain at least one tuple of microdata table. Second anonymizes microdata table, and then refines the resulting groups using public database.

Definition 4. (*k*-join-Anonymity) *A table T satisfies k-join-anonymity if for every tuple* $t \in T$ *there exist k - 1 other tuples* $t_{i1}, t_{i2}, \ldots\ldots, t_{ik-1} \in T$ *such that* $t[C] = t_{i1}[C] = t_{i2}[C] = \ldots\ldots = t_{ik-1}[C]$ *for all* $C \in QI$.

The Anonymized Table *T**. Since the quasi-identifiers might uniquely identify tuples in *T*, the table *T* is not published; it is subjected to an *anonymization procedure* and the resulting table *T** is published instead.

ALGORITHM

TOP DOWN GREEDY ALGORITHM

1. IF |T| ≤ k THEN
2. RETURN;

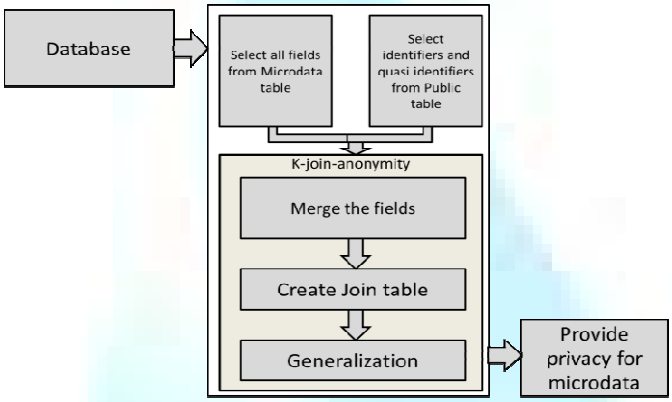
3. ELSE {
4. Partition T into two exclusive subsets T1 and T2 such that T1 and T2;
5. IF |T1| > k THEN
6. recursively partition T1;
7. IF |T2| > k THEN
8. recursively partition T2;
9. }
10. Adjust the groups so that each group has at leastk tuples;

K-JOIN-ANONYMOUS ALGORITHM

1. read quasi-identifier from MT, RT and JT is empty.
2. read quasi-identifier from PT, RT and JT is empty.
3. FOR i=1 to n DO
4. JT=(MT,PT);
5. FOR i=1 to m DO
   a) marked 0 on the Tuple of table T;
   b) read into an Tuple;
   c) FOR j=1 TO m DOto find the Tuple which containthe attribute most close to othertuple;
   d)The Tuple of the smallest mark dowith a generalization, and be integrated into the RT;
   e) Repeat the step 4 until all tuples of JTwere generalized;
6. Output the table of RT.

SYSTEM ARCHITECTURE

FIGURE 1: SYSTEM ARCHITECTURE



Definition 5. *Ananonymized table AT of join table is k-join-anonymous if the mapping of each record in join table is indistinguishable among the mapping of at least k-1 other join table tuples.*

Definition 6. (**Distance between two numeric values**) *Let D be a finite numeric domain. Then the normalized distance between two values* $v_i, v_j \in D$ *is defined as:*

$\delta_N(v_1, v_2) = |v_1 - v_2| / |D|$,

where $|D|$ is the domain size measured by the difference between the maximum and minimum values in *D*.

4.1 THE GENERALIZATION OF ATTRIBUTE VALUES

FIGURE 2.1: ZIP DOMAIN

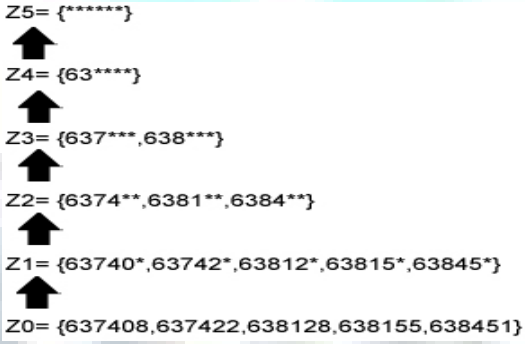
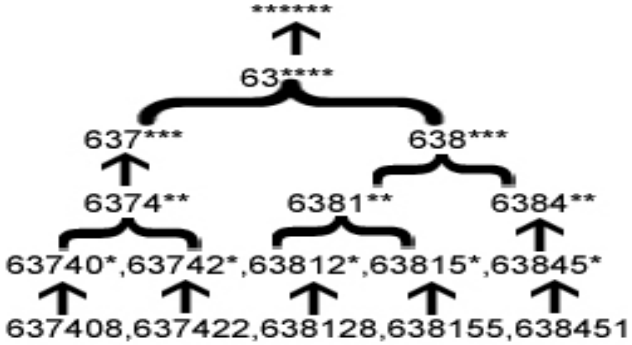
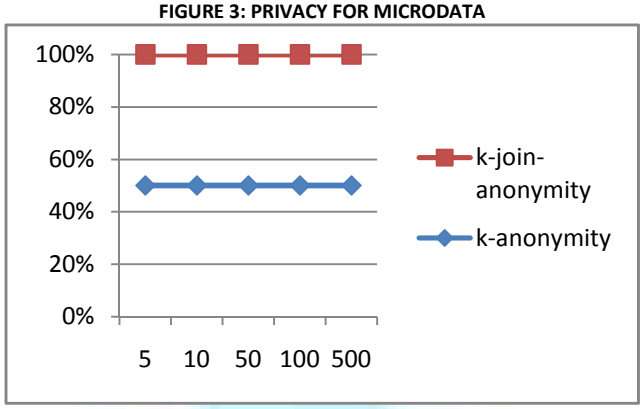


FIGURE 2.2: VALUE GENERALIZATION HIERARCHIES



On a data table, replaced the original value of attribute with another value that can indicate a larger geographical area and have the same semantic, this process is known as a generalization[6]. For example, zip= 637408 can become zip= 63740* and zip=63740* and zip=63742* can become zip=6374**, the generalization value and the original value maintain the right consistency and expand the area represented by the attribute. In relational database system, a domain are used to present of attribute a set of value that attributes assume, in order to facilitate the description of generalization on the attribute, there is need to expand the concept of attribute domain. The original table of data is as specific as possible, but in order to achieve K anonymous, it is necessary to generalize the original data, so reached the level of a more wide. After a generalization, a set of attribute value become a high-level domain. for example, in Figure 2.1 the zip code 637408 is located in the bottom of the domain Z0, generalization of the zip is refers to more widely domain, with Z1 instead of Z0, the operation can be considered from Z0 to Z1 mapping, 637408 → 63740*.

FIGURE 3: PRIVACY FOR MICRODATA



In the Figure 3. Represent the privacy for microdata in k-anonymity and k-join-anonymity. By using k-join-anonymity the information loss will be reduced and utilization of public database, microdata table join table was created and generalization is applied to join table.

5. CONCLUSION

In existing generalization algorithm creates anonymous table by using microdata table. Omission of public database leads to a high information loss. So We introduced new concept k-join-anonymity (KJA), that reduces information loss while publishing data and it is more effective generalization. KJA permits utilization of existing generalization techniques. The privacy for microdata is achieved by using k-join anonymity. In this method, information loss is reduced and public database also taken for anonymization process.

6. REFERENCES

1. D.J. Martin, D. Kifer, A. Machanavajjhala, J. Gehrke, and J.Y.Halpern, "Worst-Case Background Knowledge for Privacy-Preserving Data Publishing," Proc. IEEE Int'l Conf. Data Eng. (ICDE), pp. 126-135, 2007.
2. Dimitris Sacharidis, Kyriakos Mouratidis, and Dimitris Papadias, "k-Anonymity in the Presence of External Databases" IEEE transactions on knowledge and data engineering, vol. 22, no. 3, march 2010.
3. Jian Xu, Wei Wang, Jian Pei, Xiaoyuan Wang, Baile Shi, Ada Wai-Chee Fu " Utility-Based Anonymization Using Local Recoding", KDD'06, August 20--23, 2006.
4. L. Sweeney. k-anonymity: A model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10(5):557–570, 2002.
5. L. Sweeney. Uniqueness of simple demographics in the u.s. population. Technical report, Carnegie Mellon University, 2000
6. Mohammad Reza Zare Mirakabad, Aman Jantan, "Diversity versus Anonymity for Privacy Preservation".Proc. IEEE, pp. 978-1-4244-2328-6, 2008.
7. P. Samarati. Protecting respondents' Identities in Microdata Release," In IEEE Transactions on Knowledge and Data Engineering, 2001.
8. R.J. Bayardo and R. Agrawal, "Data Privacy through Optimal k- Anonymization," Proceedings of the 21st International conference on Data Engineering (ICDE 2005) 1084-4627/05."
9. Song Ren-jie, Lei Zhong-yue and Feng Liang-tao, "An Improved K-anonymity Algorithm Model", The 1st International Conference on Information Science and Engineering (ICISE2009)"
10. Xiaoxun Sun Hua Wang Lili Sun, "Extended K-Anonymity Models Against Attribute Disclosure", 2009 Third International Conference on Network and System Security.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application and Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you tosupply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail**infoijrcm@gmail.com** for further improvements in the interest of research.

If youhave any queries please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-

Co-ordinator

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals