

Implement L-Diversity by using Suppression Algorithm

Miss Swati Abhimanyu Nase

ME Student

Department of Computer Science & Engineering

CSMSS CHH, Shahu College of Engineering, Aurangabad, Maharashtra, India

Abstract— K-anonymity introduced due to security risk in Relational database system .To avoid identity disclosure of individuals depending upon Background knowledge attack in Role base access control system L-diverse record retrieve to maintain privacy of individual. One record in table has same Quasi identifier at least k-1 record, to implement L-diversity .This paper represent how L-diversity implemented by using suppression algorithm.

Key words: L-diversity, Relational database system, Background knowledge attack, Role base access control system, L-diversity, Quasi identifier

I. INTRODUCTION

Table1 Bank Customer Details Contains field Name, Date of birth, Phone Number and Sex. Table2 Customer Salary Details contains field Age, Date of birth, Phone Number, Sex and Salary. Age, Date of birth, Phone Number and Sex are common field in Table1 and Table2. .By knowing common fields in Table1 and Table2 by background knowledge attacker comes to knows particular person name has how much salary which is sensitive information. Some attribute like phone number which is uniquely identify individual. To avoid identity disclosure and leakage of sensitive information some information is not released such technique is called as suppression. Table3 Suppressed Data contains suppression techniques applied on attribute Phone Number in which last three digits of Phone Number is not released .It is replaced by asterisk sign.

Name	Date of birth	Phone Number	Age	Sex
Rima	19/9/88	8888888888	28	Female
Aniket	5/7/73	1818118181	42	Male
Kailas	4/3/65	2222222222	50	Male
Ambar	12/3/89	1288812888	29	Male
Pranali	2/2/94	8811188111	27	Female

Table 1: Bank Customer Details

Age	Date of birth	Phone Number	Sex	Salary
28	19/9/88	8888888888	Female	50000
42	5/7/73	1818118181	Male	30000
50	4/3/65	2222222222	Male	8000
29	12/3/89	1288812888	Male	10000
27	2/2/94	8811188111	Female	20000

Table 2: Customer Salary Details

Name	Date of birth	Phone Number	Age	Sex
Rima	19/9/88	8888888***	28	Female
Aniket	5/7/73	1818118***	42	Male
Kailas	4/3/65	2222222***	50	Male
Ambar	12/3/89	1288812***	29	Male
Pranali	2/2/94	8811188***	27	Female

Table 3: Suppressed Data

II. LITERATURE SURVEY

Privacy-Preserving Data Publishing: A Survey of Recent Developments present, what kind of data to be published

and agreement on use of published data this is known as privacy preserving data publishing .Data publisher collect record from released to public or data recipient. There are two model trusted model .In trusted model record owner willing to provide personal information to data publisher not transitive to data recipient. Data recipient could be attacker. Trustworthy person have privacy key to access data. Record linkage, attribute linkage and table linkage are example of attacker model by knowing QID of victim. Attribute linkage present in released table and seek to identify victim record for sensitive information presence or absence of victim in released table to present this privacy model is. To prevent record linkage k-anonymity proposed. One record in table has same Quasi identifier at least k-1 record have value Quasi identifier. To avoid attribute linkage l-diversity proposed that every Quasi identifier group has at least l well represented sensitive value. Attribute linkage and record linkage assume that attacker already knows victims record is in released table. Table linkages occur if an attacker confidently infers the presence or absence of victim record in released table. Generalization and suppression hide detail in Quasi identifier. In generalization replace some value by parent value in hierarchy of attribute. Suppression replaces some value with special value, indicating replaced values are not disclosed. IN multiple releases several release for different purpose. Sequential release data is released contiguously and sequentially as new information become available. Collaborative data publishing where several data publisher own different set of attribute on same set of record and want to publish the integrated data on attribute. Example of collaborative data publishing credit card bank fraud detection system. Privacy preserving tool for individual in future proposed [1]. Database Security-Concepts, Approaches and Challenges, paper focuses on data protection is important for security needed to avoid unauthorized access to data or modification. For secure outsourcing of data encryption technique is used. Discretionary access control related to function granting & revoking authorization can example here protection object are tables & views. In content based authorization manager can access only employee that work in the project that he manages. Fine grained access mechanism support access control at tuple level. RBAC model used role based access control policies of organization. Granted authorization for playing role. Advance application needed manage multimedia object, decision support technique, data mining technique. Protecting database is even difficult today. Data must be complete, correct & updated with respect to external world. Data in many cases are result of intellectual activity of individual & organization. Privacy preserving technique for data is challenge [2].

III. SUPPRESSION ALGORITHM

- 1) Get string which is to be a suppressed

- 2) Initialize variable *num_asterisk* to how many letters suppression is to be applied
- 3) Define variable *asterisk* =length of string – *num_asterisk*
- 4) *res* initializes to new string
- 5) for(int *i*=1;*i*<=*asterisk*;*i*++)
{
 res="*"
}
- Return *res*
- 6) Display output

A. How it work

Consider here attribute ten digit Phone Number is to be suppressed. Initialize variable *num_asterisk* to how many letters suppression is to be applied. Consider upon last three digit of Phone Number suppression to be applied. In line number three variable *asterisk* initialize to value store in variable *num_asterisk* subtracted from actual length of string. still for loop condition true *res* initialized to asterisk sign. When condition false return *res*. In display output on last three digits of Phone Number suppression applied means its not displayed instead of that asterisk sign placed.

IV. CONCLUSION

To maintain privacy of individual and avoid identity disclosure suppression algorithm used to implement L-diversity.

REFERENCES

- [1] B. Fung, K. Wang, R. Chen, and P. Yu, "Privacy-Preserving Data Publishing: A Survey of Recent Developments," ACM Computing Surveys, vol. 42, no. 4, article 14, 2010.
- [2] A. Rask, D. Rubin, and B. Neumann, "Implementing Row-and Cell-Level Security in Classified Databases Using SQL Server 2005," MS SQL Server Technical Center, 2005.