Journal of Information Security, 2013, 4, 101-112
http://dx.doi.org/10.4236/jis.2013.42012 Published Online April 2013 (http://www.scirp.org/journal/jis)

Attacks on Anonymization-Based Privacy-Preserving: A Survey for Data Mining and Data Publishing

Abou-el-ela Abdou Hussien[1], Nermin Hamza[2], Hesham A. Hefny[2]
[1]Department of Computer Science, Faculty of Science and Humanities, Shaqra University, Shaqra, KSA
[2]Department of Computer and Information Sciences, Institute of Statistical Studies and Research, Cairo University, Giza, Egypt
Email: abo_el_ela_2004@yahoo.com, nermin_hamza@yahoo.com, hehefny@hotmail.com

Received December 23, 2012; revised January 24, 2013; accepted February 2, 2013

ABSTRACT

Data mining is the extraction of vast interesting patterns or knowledge from huge amount of data. The initial idea of privacy-preserving data mining PPDM was to extend traditional data mining techniques to work with the data modified to mask sensitive information. The key issues were how to modify the data and how to recover the data mining result from the modified data. Privacy-preserving data mining considers the problem of running data mining algorithms on confidential data that is not supposed to be revealed even to the party running the algorithm. In contrast, privacy-preserving data publishing (PPDP) may not necessarily be tied to a specific data mining task, and the data mining task may be unknown at the time of data publishing. PPDP studies how to transform raw data into a version that is immunized against privacy attacks but that still supports effective data mining tasks. Privacy-preserving for both data mining (PPDM) and data publishing (PPDP) has become increasingly popular because it allows sharing of privacy sensitive data for analysis purposes. One well studied approach is the k-anonymity model [1] which in turn led to other models such as confidence bounding, l-diversity, t-closeness, (α,k)-anonymity, etc. In particular, all known mechanisms try to minimize information loss and such an attempt provides a loophole for attacks. The aim of this paper is to present a survey for most of the common attacks techniques for anonymization-based PPDM & PPDP and explain their effects on Data Privacy.

Keywords: Privacy; k-Anonymity; Data Mining; Privacy-Preserving Data Publishing; Privacy-Preserving Data Mining

1. Introduction

Although data mining is potentially useful, many data holders are reluctant to provide their data for data mining for the fear of violating individual privacy. In recent years, study has been made to ensure that the sensitive information of individuals cannot be identified easily. One well studied approach is the k-anonymity model [1] which in turn led to other models such as confidence bounding, l-diversity [2], (α,k)-anonymity [3], t-closeness [4]. These models assume that the data or table T contains: (1) a quasi-identifier (QID), which is a set of attributes (e.g., a QID may be {Date of birth, Zipcode, Sex}) in T which can be used to identify an individual, and (2) sensitive attributes, attributes in T which may contain some sensitive values (e.g., HIV of attribute Disease) of individuals. Often, it is also assumed that each tuple in T corresponds to an individual and no two tuples refer to the same individual. All tuples with the same QID value form an equivalence class, which we call QID-EC. The table T is said to satisfy k-anonymity if the size of every equivalence class is greater than or equal to k. The intuition of k-anonymity is to make sure that each individual is indistinguishable from other k – 1 individuals. In this paper, we present some attacks for anonymization-based PPDM & PPDP and explain their effects. The paper is organized as follows: Section 2 explains anonymity models, Section 3 presents related research directions, Section 4 discusses anonymization-based attacks, and Section 4 concludes the paper and presents future works.

2. Anonymity Models

k-anonymization techniques have been the focus of intense research in the last few years. In order to ensure anonymization of data while at the same time minimizing the information loss resulting from data modifications, several extending models are proposed, which are dis-

cussed as follows.

2.1. k-Anonymity

k-anonymity [1] is one of the most classic models, which technique that prevents joining attacks by generalizing and/or suppressing portions of the released microdata so that no individual can be uniquely distinguished from a group of size k. In the k-anonymous tables, a data set is k-anonymous ($k \geq 1$) if each record in the data set is indistinguishable from at least ($k - 1$) other records within the same data set. The larger the value of k, the better the privacy is protected. k-anonymity can ensure that individuals cannot be uniquely identified by linking attacks. Let T (*i.e*. TABLE) is a relation storing private information about a set of individuals. The attributes in T are classified in four categories: an identifier (AI), a sensitive attribute (SA), quasi-identifier attributes (QI) and other unimportant attributes. For example, we have a raw medical data set as in **Table 1**. Attributes sex, age and postcode form the quasi-identifier. Two unique patient records 1 and 2 may be re-identified easily since their combinations of sex, age and postcode are unique. The table is generalized as a 2-anonymous table as in **Table 2**. This table makes the two patients less likely to be re-identified.

However, while k-anonymity protects against identity disclosure, it does not provide sufficient protection against attribute disclosure by the homogeneous attack and the background knowledge attack.

2.2. Extending Models

Since k-anonymity does not provide sufficient protection against attribute disclosure. The paper in [2] proposes the model of l-diversity. The notion of l-diversity attempts to solve this problem by requiring that each equivalence class has at least l well-represented value for each sensitive attribute. The technology of l-diversity has some advantages than k-anonymity. Because k-anonymity dataset permits strong attacks due to lack of diversity in the sensitive attributes. In this model, an equivalence class is said to have l-diversity if there are at least l well-represented value for the sensitive attribute. Because there are semantic relationships among the attribute values, and different values have very different levels of sensitivity. An extending model called t-closeness is proposed in [3], which requires that the distribution of a sensitive attribute in any equivalence class is close to the distribution of the attribute in the overall table. That is, a table is said to have t-closeness if all equivalence classes have t-closeness. The paper in [4] extends the k-anonymity model to the (α,k)-anonymity model to limit the confidence of the implications from the quasi-identifier to a sensitive value (attribute) to within a in order to protect the sensitive information from being inferred by strong implications. After anonymization, in any equivalence class, the frequency (in fraction) of a sensitive value is no more than α. The paper in [5] proposes such a k-anonymization model for transactional databases. Assuming that the maximum knowledge of an adversary is at most m items in a specific transaction, it wants to prevent him from distinguishing the transaction from a set of k published transactions in the database. LeFevre *et al*. in [6] propose the notion of multidimensional k-anonymity [7] where data generalization is over multi-dimension at a time, and [8] extend multidimensional generalization to anonymize data for a specific task such as classification. Recently, m-invariance is introduced by Xiaokui Xiao and Yufei Tao in [9] in order to effectively limit the risk of privacy disclosure in re-publication. The paper in [10] proposes a generalization technique called HD-composition to offer protection on serial publishing with permanent sensitive values. It involves two major roles, holder and decoy. Decoys are responsible for protecting permanent sensitive value holder which is a dynamic setting. According k-anonymity does not take into account personal anonymity requirements, personalized anonymity model is also introduced in [11]. The core of the model is the concept of personalized anonymity, *i.e*., a person can specify the degree of privacy protection for her/his sensitive values.

Table 1. Raw medical data set.

AI	QI			SA
Name	**Sex**	**Age**	**Postcode**	**Illness**
Bill	**M**	**20**	**13000**	**Flu**
Ken	**M**	**24**	**13500**	**HIV**
Linda	**F**	**26**	**16500**	**Fever**
Mary	**F**	**28**	**16400**	**HIV**

Table 2. A 2-anonymos data set of Table 1.

AI	QI			SA
Name	**Sex**	**Age**	**Name**	**Sex**
Bill	**M**	**[20,24]**	**13*00**	**Flu**
Ken	**M**	**[20,24]**	**13*00**	**HIV**
Linda	**F**	**[26,28]**	**16*00**	**Fever**
Mary	**F**	**[26,28]**	**16*00**	**HIV**

3. Related Research Areas

Several polls [12,13] show that the public has an increased sense of privacy loss. Since data mining is often a key component of information systems, homeland se-

curity systems [14], and monitoring and surveillance systems [15], it gives a wrong impression that data mining is a technique for privacy intrusion. This lack of trust has become an obstacle to the benefit of the technology. For example, the potentially beneficial data mining research project, Terrorism Information Awareness (TIA), was terminated by the US Congress due to its controversial procedures of collecting, sharing, and analyzing the trails left by individuals [14].

Motivated by the privacy concerns on data mining tools, a research area called privacy-reserving data mining (PPDM) emerged in 2000 [16,17]. The initial idea of PPDM was to extend traditional data mining techniques to work with the data modified to mask sensitive information. The key issues were how to modify the data and how to recover the data mining result from the modified data. The solutions were often tightly coupled with the data mining algorithms under consideration. In contrast, privacy-preserving data publishing (PPDP) may not necessarily tie to a specific data mining task, and the data mining task is sometimes unknown at the time of data publishing. Furthermore, some PPDP solutions emphasize preserving the data truthfulness at the record level, but PPDM solutions often do not preserve such property.

PPDP Differs from PPDM in Several Major Ways as Follows

1) PPDP focuses on techniques for publishing data, not techniques for data mining. In fact, it is expected that standard data mining techniques are applied on the published data. In contrast, the data holder in PPDM needs to randomize the data in such a way that data mining results can be recovered from the randomized data. To do so, the data holder must understand the data mining tasks and algorithms involved. This level of involvement is not expected of the data holder in PPDP who usually is not an expert in data mining.

2) Both randomization and encryption do not preserve the truthfulness of values at the record level; therefore, the released data are basically meaningless to the recipients. In such a case, the data holder in PPDM may consider releasing the data mining results rather than the scrambled data.

3) PPDP primarily "anonymizes" the data by hiding the identity of record owners, whereas PPDM seeks to directly hide the sensitive data. Excellent surveys and books in randomization [16,18-23] and cryptographic techniques [17,24,25] for PPDM can be found in the existing literature.

A family of research work [26-33] called privacy-preserving distributed data mining (PPDDM) [17] aims at performing some data mining task on a set of private databases owned by different parties. It follows the principle of Secure Multiparty Computation (SMC) [34,35], and prohibits any data sharing other than the final data mining result. Clifton *et al*. [17] present a suite of SMC operations, like secure sum, secure set union, secure size of set intersection, and scalar product, that are useful for many data mining tasks. In contrast, PPDP does not perform the actual data mining task, but concerns with how to publish the data so that the anonymous data are useful for data mining. We can say that PPDP protects privacy at the data level while PPDDM protects privacy at the process level. They address different privacy models and data mining scenarios.

In the field of statistical disclosure control (SDC) [18, 36], the research works focus on privacy-preserving publishing methods for statistical tables. SDC focuses on three types of disclosures, namely identity disclosure, attribute disclosure, and inferential disclosure [37]. Identity disclosure occurs if an adversary can identify a respondent from the published data. Revealing that an individual is a respondent of a data collection may or may not violate confidentiality requirements. Attribute disclosure occurs when confidential information about a respondent is revealed and can be attributed to the respondent. Attribute disclosure is the primary concern of most statistical agencies in deciding whether to publish tabular data [37]. Inferential disclosure occurs when individual information can be inferred with high confidence from statistical information of the published data. Some other works of SDC focus on the study of the non-interactive query model, in which the data recipients can submit one query to the system. This type of non-interactive query model may not fully address the information needs of data recipients because, in some cases, it is very difficult for a data recipient to accurately construct a query for a data mining task in one shot. Consequently, there are a series of studies on the interactive query model [38-40], in which the data recipients, including adversaries, can submit a sequence of queries based on previously received query results. The database server is responsible to keep track of all queries of each user and determine whether or not the currently received query has violated the privacy requirement with respect to all previous queries. One limitation of any interactive privacy-preserving query system is that it can only answer a sublinear number of queries in total; otherwise, an adversary (or a group of corrupted data recipients) will be able to reconstruct all but $1 - o(1)$ fraction of the original data [41], which is a very strong violation of privacy. When the maximum number of queries is reached, the query service must be closed to avoid privacy leak. In the case of the non-interactive query model, the adversary can issue only one query and, therefore, the non-interactive query model cannot achieve the same degree of privacy defined by Introduction the interactive

model. One may consider that privacy-reserving data publishing is a special case of the non-interactive query model.

4. Anonimization-Based Attacks

In this paper, we study the case where the adversary has some additional knowledge about the mechanism involved in the anonymization and launches an attack based on this knowledge. We distinguish heir between both PPDM and PPDP attacks.

4.1. Privacy-Preserving Data Publishing PPDP Attacks

In this section we present Attacks for anonimization-based attacks in privacy-preserving data publishing and we study mainly minimality attack.

Minimality Attack

In **Table 3(a)**, assume that the QID values of q1 and q2 can be generalized to Q and assume only one sensitive attribute "disease", in which HIV is a sensitive value. For example, q1 may be {Nov 1930, Z3972, M}, q2 may be {Dec 1930, Z3972, M} and Q is {Nov/Dec 1930, Z3972, M}. (Note that q1 and q2 may also be generalized values). A tuple associated with HIV is said to be a sensitive tuple. For each equivalence class, at most half of the tuples are sensitive. Hence, the table satisfies 2-diversity. As observed in LeFevre *et al*. [2005], existing approaches of anonymization for data publishing have an implicit principle: "For any anonymization mechanism, it is desirable to define some notion of minimality". Intuitively, a k-anonymization should not generalize, suppress, or dis- tort the data more than it is necessary to achieve k-ano- nymity". Based on this minimality principle, **Table 3(a)** will not be generalized. In fact the aforesaid notion of minimality is too strong since almost all known anonymization problems for data publishing are NP-hard, many existing algorithms are heuristical and only attain local minima. We shall later give a more relaxed notion of the minimality principle in order to cover both the optimal as well as the heuristical algorithms. For now, we assume that mimimality principle means that a QID-EC will not be generalized unnecessarily. Next, consider a slightly different table, **Table 3(b)**. Here, the set of tuples for q1 violates 2-diversity because the proportion of the sensitive tuples is greater than 1/2. Thus, this table will be anonymized to a generalized table by generalizing the QID values as shown in **Table 3(c)** by global recoding [11]. In global recoding, all occurrences of an attribute value are recoded to the same value. If local recoding [Sweeney, 2002a; Aggarwal *et al*., 2005a, 2005b] is adopted, occurrences of the same value of an attribute may be recoded to different values. Such an anonymization is shown in **Table 3(d)**. These anonymized tables satisfy 2-diversity. The question we are interested in is whether these tables really protect individual privacy. In most previous works [Sweeney, 2002b; LeFevre *et al*., 2006, 2005; Xiao and Tao, 2006b], the knowledge of the adversary involves an external table T^e. such as a voter registration list that maps QIDs to individuals. As in many previous works, we assume that each tuple in T^e maps to one individual and no two tuples map to the same individual. The same is also assumed in the table T to be published. Let us first consider the case when T and T^e are mapped to the same set of individuals. **Table 4(a)** is an example of T^e. Assume further that the adversary knows the goal of 2-diversity, s/he also knows whether it is a global or local recoding, and **Table 4(a)** is available as the external table T^e. With the notion of minimality in anonymization, the adversary reasons as follows: From the published **Table 3(c)**, there are 2 sensitive tuples in total. From T^e, there are 2 tuples with QID = q1 and 5 tuples with QID = q2. Hence, the equivalence class for q2 in the original table must already satisfy 2-diversity, because even if both sensitive tuples have QID = q2, the proportion of sensitive values in the class for q2 is only 2/5.

Table 3. 2-diversity: Global and local recoding.

QID	**Disease**	QID	Disease	**QID**	**Disease**	QID	Disease
q1	**HIV**	q1	HIV	**Q**	**HIV**	Q	HIV
q1	**non-sensitive**	q1	HIV	**Q**	**HIV**	Q	HIV
q2	**HIV**	q2	non-sensitive	**Q**	**non-sensitive**	Q	non-sensitive
q2	**non-sensitive**	q2	non-sensitive	**Q**	**non-sensitive**	Q	non-sensitive
q2	**non-sensitive**	q2	non-sensitive	**Q**	**non-sensitive**	q2	non-sensitive
q2	**non-sensitive**	q2	non-sensitive	**Q**	**non-sensitive**	q2	non-sensitive
q2	**non-sensitive**	q2	non-sensitive	**Q**	**non-sensitive**	q2	non-sensitive
(a)	**Good table**	(b)	Bad table	**(c)**	**Global**	(d)	Local

Table 4. T^e: External table available to the adversary.

QID	**QID**	**Name**	QID	**QID**	**Name**
q1	**q1**	**Andre**	q1	**q1**	**Andre**
q1	**q1**	**Kim**	q1	**q1**	**Kim**
q2	**q2**	**Jeremy**	q2	**q2**	**Jeremy**
q2	**q2**	**Victoria**	q2	**q2**	**Victoria**
q2	**q2**	**Ellen**	q2	**q2**	**Ellen**
q2	**q2**	**Sally**	q2	**q2**	**Sally**
q2	**q2**	**Ben**	q2	**q2**	**Ben**
q4	**q4**	**Tim**			
q4	**q4**	**Joseph**			
(a) Individual QID	(b)	multiset	**(c) Individual QID**	(d)	multiset

Since generalization has taken place, at least one equivalence class in the original table T must have violated 2-diversity, because otherwise no generalization will take place according to minimality. The adversary concludes that q1 has violated 2-diversity, and that is possible only if both tuples with QID = q1 have a disease value of "HIV". The adversary therefore discovers that Andre and Kim are linked to "HIV". In some previous works, it is assumed that the set of individuals in the external table T^e can be a superset of that for the published table. **Table 4(c)** shows such a case, where there is no tuple for Tim and Joseph in **Table 3(a)** and **Table 3(b)**. If it is known that q4 cannot be generalized to Q (e.g., q4 = {Nov 1930, Z3972, F} and Q = {Jan/Feb 1990, Z3972, M}), then the adversary can be certain that the tuples with QID = q4 are not in the original table. Thus, the tuples with QID = q4 in Te do not have any effect on the previous reasoning of the adversary and, therefore, the same conclusion can be drawn. We call such an attack based on the minimality principle a minimality attack.

***Observation* 1.** If a table T is anonymized to T^* which satisfies l-diversity, it can suffer from a minimality attack. This is true for both global and local recoding and for the cases when the set of individuals related to T^e is a superset of that related to T. In the preceding example, some values in the sensitive attribute Disease are not sensitive. Would it help if all values in the sensitive attributes are sensitive? In the tables in **Table 5**, we assume that all values for Disease are sensitive. **Table 5(a)** satisfies 2-diversity but **Table 5(b)** does not. Suppose anonymization of **Table 5(b)** results in **Table 5(c)** by global recoding and **Table 5(d)** by local recoding.

The adversary is armed with the external table **Table 4(c)** and the knowledge of the goal of 2-diversity, s/he can launch an attack by reasoning as follows: With 5 tuples for QID = q2 and each sensitive value appearing at most twice, there cannot be any violation of 2-diversity for the tuples with QID = q2. There must have been a violation for QID = q1. For a violation to take place, both tuples with QID = q1 must be linked to the same disease. Since HIV is the only disease that appears twice, Andre and Kim must have contracted HIV.

***Observation* 2.** Minimality attack is possible whether the sensitive attribute contains non-sensitive values or not. Recall that the intended objective of 2-diversity is to make sure that an adversary cannot deduce with a probability above 1/2 that an individual is linked to any sensitive value. Thus, the published tables violate this objective. The previous attacks to Andre would also be successful if the knowledge of the external table **Table 4(a)** is replaced by that of a multiset of the QID values as shown in **Table 4(b)** plus the QID value of Andre; or if **Table 4(c)** is replaced by the multiset in **Table 4(d)** plus the QID value of Andre. Note that the multisets in **Tables 4(b)** and **(d)** are inherently available in the published data if the bucketization technique as in Xiao and Tao [2006a], Zhang *et al*. [2007], or Martin *et al*. [2007] is used.

***Observation* 3.** The minimality attacks to an individual t would also be successful if the knowledge of the external table T^e (which is either a superset of individuals of the published table or not) is replaced by that of a multiset of the QID values of the external table T^e plus the QID value of t. A strong requirement of 3-diversity is used to achieve the original intended requirement of 2-diversity.

It is natural to ask whether there is a privacy breach if the data publisher generalizes the table a little more than minimal. In this case, we say that the anonymization algorithm follows a near to minimality principle. Suppose the intended objective is to generate a table which satisfies a privacy requirement of 2-diversity. Under the near

Table 5. 2-diversity (where all values in Disease are sensitive): Global and local recoding.

Disease	QID	**Disease**	**QID**	Disease	QID	**Disease**	**QID**
HIV	Q	**HIV**	**Q**	HIV	q1	**HIV**	**q1**
HIV	Q	**HIV**	**Q**	HIV	q1	**Lung Cancer**	**q1**
Gallstones	Q	**Gallstones**	**Q**	Gallstones	q2	**Gallstones**	**q2**
Lung Cancer	Q	**Lung Cancer**	**Q**	Lung Cancer	q2	**HIV**	**q2**
Ulcer	q2	**Ulcer**	**Q**	Ulcer	q2	**Ulcer**	**q2**
Alzheimer	q2	**Alzheimer**	**Q**	Alzheimer	q2	**Alzheimer**	**q2**
Diabetes	q2	**Diabetes**	**Q**	Diabetes	q2	**Diabetes**	**q2**
Ulcer	q4	**Ulcer**	**q4**	Ulcer	q4	**Ulcer**	**q4**
Alzheimer	q4	**Alzheimer**	**q4**	Alzheimer	q4	**Alzheimer**	**q4**
(a)	**Good table**	(b)	Bad table	**(c)**	**Global**	(d)	Local

to minimality principle, the publisher generates a table which satisfies a stronger privacy requirement of 3-diversity. Again we assume that the adversary knows that the algorithm adopted guarantees 3-diversity while minimizing the information loss. Does a published table which satisfies 3-diversity guarantee that the probability that an individual is linked to a sensitive value is at most 1/2? The answer is interestingly no. Consider **Table 6**. Suppose our original intended privacy requirement is 2-diversity because we want to guarantee that the probability that an individual is linked to a sensitive value is at most 1/2. Based on the near to minimality principle, a stronger 3-diversity is attained instead. **Table 6(a)** satisfies 3-diversity but **Table 6(b)** does not. Thus, **Tables 6(c)** and **6(d)** are generated by global recoding and local recoding, respectively. By similar arguments, with the knowledge of a strong requirement 3-diversity and **Table 6(c)**, the adversary can also deduce that the probability that an individual with QID value = q1 is equal to 2/3 which is greater than the intended maximum disclosure probability of 1/2. This is because the two HIV values must be linked to the tuples with QID = q1. Otherwise, there will be no violation of 3-diversity and there is no need for generalization. Similar arguments can be made to **Table 6(d)**. We call this kind of attack the near-to-minimality attack.

***Observation* 4.** Near-to-minimality attack is possible when the anonymization algorithm follows the near to minimality principle. From the preceding discussion, we described the attack by minimality and the attack by near-to-minimality are successful under the principles of minimality principle and near-to-minimality principles used in the anonymization algorithm. Both are based on some knowledge about the algorithm, let us call an attack based on such knowledge an attack by mechanism. Hence minimality or near-minimality attack are under this bigger class of attack.

4.2. Privacy-Preserving Data Mining (PPDM) Attacks

Various attacks are addressed from a privacy-preserving perspective. In the following subsections the most common attacks are discussed.

4.2.1. Background Knowledge Attack

Recently, Xiao and Tao [42] introduced Anatomy as an alternative anonymization technique to generalization. Anatomy releases all the quasi-identifier and sensitive data directly into two separate tables. For example, the original table shown in **Table 7** is decomposed into two tables, the quasi-identifier table (QIT) in **Table 8(a)** and the sensitive table (ST) in **Table 8(b)**. The QIT table and the ST table are then released. The authors also proposed an anatomizing algorithm to compute the anatomized tables. The algorithm first hashes the records into buckets based on the sensitive attribute, *i.e*., records with the same sensitive values are in the same bucket. Then the algorithm iteratively obtains the ! buckets that currently have the largest number of records and selects one record from each of the ! buckets to form a group. Each remaining record is then assigned to an existing group.

We show background knowledge attack on the anatomized tables. Suppose Alice knows that Bob's record belongs to the first group in **Table 8(b)** where the two sensitive values are "prostate cancer" and "ovary cancer", then Alice immediately knows that Bob has "prostate cancer". The apparent diversity does not help provide any privacy, because certain values can be easily eliminated. This problem is particularly acute in the Anatomy approach. The anatomizing algorithm randomly picks records and groups them together (rather than grouping

Table 6. Illustration of near to minimality principle.

Disease	QID	**Disease**	**QID**	Disease	QID	**Disease**	**QID**
HIV	Q	**HIV**	**Q**	HIV	q1	**HIV**	**q1**
HIV	Q	**HIV**	**Q**	HIV	q1	**non-sensitive**	**q1**
non-sensitive	Q	**non-sensitive**	**Q**	non-sensitive	q1	**non-sensitive**	**q1**
non-sensitive	Q	**non-sensitive**	**Q**	non-sensitive	q2	**HIV**	**q2**
non-sensitive	Q	**non-sensitive**	**Q**	non-sensitive	q2	**non-sensitive**	**q2**
non-sensitive	Q	**non-sensitive**	**Q**	non-sensitive	q2	**non-sensitive**	**q2**
non-sensitive	q2	**non-sensitive**	**Q**	non-sensitive	q2	**non-sensitive**	**q2**
non-sensitive	q2	**non-sensitive**	**Q**	non-sensitive	q2	**non-sensitive**	**q2**
non-sensitive	q2	**non-sensitive**	**Q**	non-sensitive	q2	**non-sensitive**	**q2**
(a)	**Good table**	(b)	Bad table	**(c)**	**Global**	(d)	Local

Table 7. Original patients table.

Disease	Sex	Age	ZIP Code	
Ovarian Cancer	**F**	**29**	**47677**	**1**
Ovarian Cancer	**F**	**22**	**47602**	**2**
Prostate Cancer	**M**	**27**	**47678**	**3**
Flu	**M**	**43**	**47905**	**4**
Heart Disease	**F**	**52**	**47909**	**5**
Heart Disease	**M**	**47**	**47906**	**6**
Heart Disease	**M**	**30**	**47605**	**7**
Flu	**M**	**36**	**47673**	**8**
Flu	**M**	**32**	**47607**	**9**

Table 8. (a) The quasi-identifier table (QIT); (b) The sensitive table (ST).

(a)

Disease	Sex	Age	ZIP Code	
1	**F**	**29**	**47677**	**1**
1	**F**	**22**	**47602**	**2**
1	**M**	**27**	**47678**	**3**
2	**M**	**43**	**47905**	**4**
2	**F**	**52**	**47909**	**5**
2	**M**	**47**	**47906**	**6**
3	**M**	**30**	**47605**	**7**
3	**M**	**36**	**47673**	**8**
3	**M**	**32**	**47607**	**9**

(b)

Group-ID	Disease	Count
1	**Ovarian Cancer**	**2**
1	**Prostate Cancer**	**1**
2	**Flu**	**1**
2	**Heart Disease**	**2**
3	**Heart Disease**	**1**
3	**Flu**	**2**

records with similar quasi-id values together). Therefore, it is likely that one may be grouping records with incompatible sensitive attribute values together.

4.2.2. Unsorted Matching Attack

This attack is based on the order in which tuples appear in the released table. While we have maintained the use of a relational model, and so the order of tuples cannot be assumed, in real-world use this is often a problem. It can be corrected of course, by randomly sorting the tuples of the solution. Otherwise, the release of a related table can leak sensitive information.

From **Figure 1** we can see that this attack is based on the order in which tuples appear in the released table.

Solution: Random shuffling of rows.

4.2.3. Complementary Release Attack

It is more common that the attributes that constitute the quasi-identifier are themselves a subset of the attributes released. As a result, when a k-minimal solution, which we will call table T is released, it should be considered as joining other external information. Therefore, subsequent releases of generalizations of the same privately held information must consider all of the released attributes of T a quasi-identifier to prohibit linking on T, unless of course, subsequent releases are themselves generalizations of T.

From **Figure 2** we find that Different releases can be linked together to compromise k-anonymity.

Solution:

1) Consider all of the released tables before release the new one, and try to avoid linking.

2) Other data holders may release some data that can be used in this kind of attack. Generally, this kind of attack is hard to be prohibited completely.

Race	Zip	Race	Zip	Race	Zip
Asian	**02138**	**Person**	**02138**	**Asian**	**02130**
Asian	**02139**	**Person**	**02139**	**Asian**	**02130**
Asian	**02141**	**Person**	**02141**	**Asian**	**02140**
Asian	**02142**	**Person**	**02142**	**Asian**	**02140**
Black	**02138**	**Person**	**02138**	**Black**	**02130**
Black	**02139**	**Person**	**02139**	**Black**	**02130**
Black	**02141**	**Person**	**02141**	**Black**	**02140**
Black	**02142**	**Person**	**02142**	**Black**	**02140**
White	**02138**	**Person**	**02138**	**White**	**02130**
White	**02139**	**Person**	**02139**	**White**	**02130**
White	**02141**	**Person**	**02141**	**White**	**02140**
White	**02142**	**Person**	**02142**	**White**	**02140**
PT		**GT1**		**GT2**	

Figure 1. Demonstrate unsorted matching attack.

4.2.4. Temporal Attack

Data collections are dynamic. Tuples are added, changed, and removed constantly. As a result, releases of generalized data over time can be subject to a temporal inference attack.

From **Figures 3(a)**, **(b)** and **(c)**, we see that adding or removing tuples may compromise k-anonymity protection.

Solution: Subsequent releases must use the already released table.

4.2.5. Homogeneity Attack and Background Knowledge Attack

In this subsection we present two major attacks, the homogeneity attack and background knowledge attack [43], along with unsorted matching attack, complementary release attack and temporal attack, and we show that how they can be used to compromise a k-anonymous dataset.

Problem	ZIP	Gender	Birth Date	Race	Problem	ZIP	Gender	Birth Date	Race
Short of breath	02141	male	1965	black	Short of breath	02141	male	1965	black
Chest pain	02141	male	1965	black	Chest pain	02141	male	1965	black
Painful eye	02138	female	1965	black	Painful eye	0213*	female	1965	Person
wheezing	02138	female	1965	black	wheezing	0213*	female	1965	person
obesity	02138	female	1964	black	obesity	02138	female	1964	black
Chest pain	02138	female	1964	black	Chest pain	02138	female	1964	black
Short of breath	02138	male	1960-69	white	Short of breath	0213*	male	1964	White
hypertension	02139	human	1960-69	white	hypertension	0213*	female	1965	person
obesity	02139	human	1960-69	white	obesity	0213*	male	1964	white
fever	02139	human	1960-69	white	fever	0213*	male	1964	white
vomiting	02138	male	1960-69	white	vomiting	02138	male	1967	white
backpain	02138	male	1960-69	white	backpain	02138	male	1967	white
		GT1					GT3		

Problem	ZIP	Gender	Birth Date	Race	Problem	ZIP	Gender	Birth Date	Race
Short of breath	02141	male	9/20/1965	black	Short of breath	02141	male	1965	black
Chest pain	02141	male	2/14/1965	black	Chest pain	02141	male	1965	black
Painful eye	01238	female	10/23/1965	black	Painful eye	02138	female	1965	black
wheezing	01238	female	8/24/1965	black	wheezing	02138	female	1965	black
obesity	02138	female	11/7/1964	black	obesity	02138	female	1964	black
Chest pain	02138	female	12/1/1964	black	Chest pain	02138	female	1964	black
Short of breath	02139	male	10/23/1964	White	Short of breath	02138	male	1964	white
hypertension	02139	female	3/15/1965	White	hypertension	02139	female	1965	white
obesity	02139	male	8/13/1964	white	obesity	02139	male	1964	white
fever	02139	male	5/5/1964	white	fever	02139	male	1964	white
vomiting	02138	male	2/13/1967	white	vomiting	02138	male	1967	white
backpain	02138	male	3/21/1967	white	backpain	02138	male	1967	white
		PT					LT		

Figure 2. Different releases for Micro-Data.

(a)

Problem	ZIP	Gender	Birth Date	Race
Short of breath	02141	male	9/20/1965	black
Chest pain	02141	male	2/14/1965	black
Painful eye	01238	female	10/23/1965	black
wheezing	01238	female	8/24/1965	black
obesity	02138	female	11/7/1964	black
Chest pain	02138	female	12/1/1964	black
Short of breath	02139	male	10/23/1964	White
hypertension	02139	female	3/15/1965	White
obesity	02139	male	8/13/1964	white
fever	02139	male	5/5/1964	white
vomiting	02138	male	2/13/1967	white
back pain	02138	male	3/21/1967	white

PT

(b)

Problem	ZIP	Gender	Birth Date	Race
Short of breath	02141	male	1965	black
Chest pain	02141	male	1965	black
Painful eye	0213*	female	1965	Person
Wheezing	0213*	female	1965	person
Obesity	02138	female	1964	black
Chest pain	02138	female	1964	black
Short of breath	0213*	male	1964	White
Hypertension	0213*	female	1965	person
Obesity	0213*	male	1964	white
Fever	0213*	male	1964	white
Vomiting	02138	male	1967	white
back pain	02138	male	1967	white

GT1

(c)

Problem	ZIP	Gender	Birth Date	Race
Short of breath	02141	male	1965	black
Chest pain	02141	male	1965	black
Painful eye	02138	female	1965	black
wheezing	02138	female	1965	black
obesity	02138	female	1964	black
Chest pain	02138	female	1964	black
Short of breath	02138	male	1960-69	white
hypertension	02139	human	1960-69	white
obesity	02139	human	1960-69	white
fever	02139	human	1960-69	white
vomiting	02138	male	1960-69	white
back pain	02138	male	1960-69	white

Figure 3. Adding or removing tuples; (a) black 9/7/65 male 02139 headache, black 11/4/65 male 02139 rash; (c) black 1965 male 02139 rash; black 1965 male 02139 headache.

So here new definition arise l-diversity. l-diversity provides privacy even when the data publisher does not know what kind of knowledge is possessed by the adversary. The main idea behind l-diversity is the requirement that the values of the sensitive attributes are well-represented in each group.

Even when sufficient care is taken to identify the QI, the k-anonymity is still vulnerable to attacks. The common attacks are unsorted matching attacks, complementary release attacks and temporal attacks. Fortunately, these attacks can be prevented by some best practices. But the two major attacks, Homogeneity and Background attacks disclose the individuals' sensitive information. K-anonymity does not protect against attacks based on background knowledge because k-anonymity can create groups that leak information.

***Observation*:** k-anonymity does not provide privacy in case of Homogeneity and Background attacks.

***Homogeneity Attack*:** Suppose A and B are enemies and A wants to infer B's medical status which is present in **Table 9**. A knows B's ZIP Code is 13053 and his age is 35. So using this knowledge A knows that B's records belong from record no. 9,10,11,12 have Cancer. So A concludes that B has Cancer. This situation or attack is implies that k-anonymity can create groups which are responsible for leakage of information. This happens due to the lack of diversity in the sensitive attribute. This problem suggests that in addition to k-anonymity, the disinfected table should also ensure "diversity" all tuples that share the same values of their quasi-identifiers should have diverse values for their sensitive attributes.

Background Knowledge Attack: Suppose C and D are two aggressive neighbors and C wants to infer D's private data, let the medical status, from the private table PT. **Table 9** shows a 4-anonymous private table with patient micro data which satisfies k-anonymity. So for a single value, C finds 3 more values. So if he wants to infer D's medical status, he has four options for disease. This is k-anonymity principle. But C knows some general details about D as his ZIP Code is 14853 and age above 50. So using these values as quasi-identifiers, C concludes that D's record is present in records 5,6,7,8. But here C has three options of disease, Cancer, Heart Disease and Viral infection. Here C uses his background knowledge and concludes that D has Heart Disease because D has low blood pressure and he avoids fatty meals.

So, we can say that k-anonymity does not protect against attacks based on background knowledge. We have demonstrated (using the homogeneity and background knowledge attacks) that a k-anonymous table may disclose sensitive information. Since both of these attacks are plausible in real life, we need a stronger definition of privacy that takes into account diversity and background knowledge. The k-anonymity may suffer with this aspect also.

Table 9. 4-anonymous inpatient microdata.

SENSITIVE	NONSENSITIVE			S. NO
Medical Status	Nationality	Age	Zip Code	
Heart Disease	*	<30	130**	1
Heart Disease	*	<30	130**	2
Viral Infection	*	<30	130**	3
Viral Infection	*	<30	130**	4
Cancer	*	≥40	1485*	5
Heart Disease	*	≥40	1485*	6
Viral Infection	*	≥40	1485*	7
Viral Infection	*	≥40	1485*	8
Cancer	*	3*	130**	9
Cancer	*	3*	130**	10
Cancer	*	3*	130**	11
Cancer	*	3*	130**	12

5. Conclusion

This paper presents a survey for most of the common attacks techniques for anonymization-based PPDM & PPDP and explains their effects on Data Privacy. k-anonymity is used for security of respondents identity and decreases linking attack in the case of homogeneity attack a simple k-anonymity model fails and we need a concept which prevent from this attack solution is l-diversity. All tuples are arranged in well represented form and adversary will divert to l places or on l sensitive attributes. l-diversity limits in case of background knowledge attack because no one predicts knowledge level of an adversary. It is observe that using generalization and suppression we also apply these techniques on those attributes which doesn't need this extent of privacy and this leads to reduce the precision of publishing table. e-NSTAM (extended Sensitive Tuples Anonymity Method) [44] is applied on sensitive tuples only and reduces information loss, this method also fails in the case of multiple sensitive tuples. Generalization with suppression is also the causes of data lose because suppression emphasize on not releasing values which are not suited for k factor. Future works in this front can include defining a new privacy measure along with l-divesity for multiple sensitive attribute and we will focus to generalize attributes without suppression using other techniques which are used to achieve k-anonymity because suppression leads to reduce the precision of publishing table.

REFERENCES

[1] P. Samarati and L. Sweeney, "Protecting Privacy When Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression," Technical Report SRI-CSL-98-04, 1998.

[2] A. Machanavajjhala, J. Gehrke, *et al*., "l -Diversity: Privacy beyond k-Anonymity," *Proceeding of ICDE*, April 2006.

[3] N. Li, T. Li and S. Venkatasubramanian, "t-Closeness: Privacy Beyond k-Anonymity and l-Diversity," *Proceedings of ICDE*, 2007, pp. 106-115.

[4] R. C. Wong, J. Li, A. W. Fu, *et a1*., "(α,k)-Anonymity: An Enhaned k-Anonymity Model for Privacy-Preserving Data Publishing," In: *Proceedings of the* 12*th ACM SIGKDD*, ACM Press, New York, 2006, pp. 754-759.

[5] M. Terrovitis, N. Mamoulis and Kalnis, "Privacy Preserving Anonymization of Set-Valued Data," *VLDB*, Auckland, 2008, pp. 115-125.

[6] K. LeFevre, D. J. DeWitt and R. Ramakrishnan, "Incognito: Efficient Full-Domain k-Anonymity," In: *Proceedings of the ACM SIGMOD International Conference on Management of Data*, Baltimore, June 2005, pp. 49-60.

[7] X. Ye, L. Jin and B. Li, "A Multi-Dimensional K-Anonymity Model for Hierarchical Data, Electronic Commerce and Security," 2008 *International Symposium*, Beijing, August 2008, pp. 327-332.

[8] K. LeFevre, D. J. DeWitt and R. Ramakrishnan, "Workload-Aware Anonymization," *Proceedings of the* 12*th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Philadelphia, August 2006, pp. 277-286. doi:10.1145/1150402.1150435

[9] X. Xiao and Y. Tao, "M-Invariance: Towards Privacy-Preserving Re-Publication of Dynamic Datasets," In: *Proceedings of SIGMOD*, ACM Press, New York, 2007, pp. 689-700.

[10] Y. Bu, A. Wai-Chee Fu, *et al.*, "Privacy-Preserving Serial Data Publishing By Role Composition," *VLDB*, Auckland, 2008, pp. 845-856.

[11] X. Xiao and Y. Tao, "Personalized Privacy Preservation, Proceedings of ACM Conference on Management of Data (SIGMOD)," ACM Press, New York, 2006, pp. 785-790.

[12] "Business for Social Responsibility," BSR Report on Privacy, 1999. http://www.bsr.org/

[13] B. Krishnamurthy, "Privacy vs. Security in the Aftermath of the September 11 Terrorist Attacks," November 2001. http://www.scu.edu/ethics/publications/briefings/privacy.html

[14] J. W. Seifert, "Data Mining and Homeland Security: An Overview," CRS Report for Congress, (RL31798), January 2006. http://www.fas.org/sgp/crs/intel/RL31798.pdf

[15] T. Fawcett and F. Provost, "Activity Monitoring: Noticing Interesting Changes in Behavior," *Proceedings of the 5th ACM International Conference on Knowledge Discovery and Data Mining* (*SIGKDD*), San Diego, 1999, pp. 53-62. doi:10.1145/312129.312195

[16] R. Agrawal and R. Srikant, "Privacy-Preserving Data Mining," *Proceedings of ACM International Conference on Management of Data* (*SIGMOD*), Dallas, 2000, pp. 439-450.

[17] C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin and M. Y. Zhu, "Tools for Privacy-Preserving Distributed Data Mining," *ACM SIGKDD Explorations Newsletter*, Vol. 4, No. 2, 2002, pp. 28-34. doi:10.1145/772862.772867

[18] N. R. Adam and J. C. Wortman, "Security Control Methods for Statistical Databases," *ACM Computer Surveys*, Vol. 21, No. 4, 1989, pp. 515-556. doi:10.1145/76894.76895

[19] S. Agrawal and J. R. Haritsa, "A Framework for High-Accuracy Privacy-Preserving Mining," *Proceedings of the* 21*st IEEE International Conference on Data Engineering* (*ICDE*), Tokyo, April 2005, pp. 193-204. doi:10.1109/ICDE.2005.8

[20] A. Evfimievski, "Randomization in Privacy-Preserving Data Mining," *ACM SIGKDD Explorations Newsletter*, Vol. 4, No. 2, 2002, pp. 43-48. doi:10.1145/772862.772869

[21] K. Liu, H. Kargupta and J. Ryan, "Random Projection-Based Multiplicative Perturbation for Privacy-Preserving Distributed Data Mining," *IEEE Transactions on Knowledge and Data Engineering* (*TKDE*), Vol. 18, No. 1, 2006, pp. 92-106. doi:10.1109/TKDE.2006.14

[22] A. Shoshani, "Statistical Databases: Characteristics, Problems and Some Solutions," *Proceedings of the* 8*th Very Large Data Bases* (*VLDB*), Mexico City, September 1982, pp. 208-213.

[23] V. S. Verykios, E. Bertino, I. N. Fovino, L. P. Provenza, Y. Saygin and Y. Theodoridis, "State-of-the-Art in Privacy Preserving Data Mining," *ACM SIGMOD Record*, Vol. 3, No. 1, 2004, pp. 50-57. doi:10.1145/974121.974131

[24] B. Pinkas, "Cryptographic Techniques for Privacy-Preserving Data Mining," *ACM SIGKDD Explorations Newsletter*, Vol. 4, No. 2, 2002, pp. 12-19. doi:10.1145/772862.772865

[25] J. Vaidya, C. W. Clifton and M. Zhu, "Privacy-Preserving Data Mining," 2006.

[26] W. Du, Y. S. Han and S. Chen, "Privacy-Preserving Multivariate Statistical Analysis: Linear Regression and Classification," *Proceedings of the SIAM International Conference on Data Mining* (*SDM*), Florida, 2004.

[27] W. Du and Z. Zhan, "Building Decision Tree Classifier on Private Data," *Workshop on Privacy*, *Security*, *and Data Mining at the* 2002 *IEEE International Conference on Data Mining*, Maebashi City, December 2002.

[28] A. W. C. Fu, R. C. W. Wong and K. Wang, "Privacy-Preserving Frequent Pattern Mining across Private Databases," *Proceedings of the* 5*th IEEE International Conference on Data Mining* (*ICDM*), Houston, November 2005, pp. 613-616.

[29] M. Kantarcioglu and C. Clifton, "Privacy-Preserving Data Mining of Association Rules on Horizontally Partitioned Data," *IEEE Transactions on Knowledge and Data Engineering* (*TKDE*), Vol. 16, No. 9, 2004, pp. 1026-1037. doi:10.1109/TKDE.2004.45

[30] M. Kantarcioglu and C. Clifton, "Privately Computing a

Distributed K-Nn Classifier," *Proceedings of the 8th European Conference on Principles and Practice of Knowledge Discovery in Databases* (*PKDD*), Pisa, September 2004, pp. 279-290.

[31] J. Vaidya and C. Clifton, "Privacy-Preserving Association Rule Mining in Vertically Partitioned Data," *Proceedings of the 8th ACM International Conference on Knowledge Discovery and Data Mining* (*SIGKDD*), Edmonton, 2002. pp. 639-644.

[32] J. Vaidya and C. Clifton, "Privacy-Preserving k-Means Clustering over Vertically Partitioned Data," *Proceedings of the 9th ACM International Conference on Knowledge Discovery and Data Mining* (*SIGKDD*), Washington, 2003, pp. 206-215.

[33] Z. Yang, S. Zhong and R. N. Wright, "Privacy-Preserving Classification of Customer Data without Loss of Accuracy," *Proceedings of the 5th SIAM International Conference on Data Mining* (*SDM*), Newport Beach, 2005, pp. 92-102.

[34] A. C. Yao, "Protocols for Secure Computations," *Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science*, Washington DC, 1982, pp. 160-164.

[35] A. C. Yao, "How to Generate and Exchange Secrets," Proceedings of the 27*th Annual IEEE Symposium on Foundations of Computer Science*, 1986, pp. 162-167.

[36] R. Brand, "Microdata Protection through Noise Addition," *Inference Control in Statistical Databases*, *From Theory to Practice*, London, 2002, pp. 97-116.

[37] Confidentiality and Data Access Committee, "Report on Statistical Disclosure Limitation Methodology," Technical Report 22, Office of Management and Budget, December 2005.

[38] A. Blum, C. Dwork, F. McSherry and K. Nissim, "Practical Privacy: The Sulq Framework," *Proceedings of the 24th ACM Symposium on Principles of Database Systems* (*PODS*), Baltimore, June 2005, pp. 128-138.

[39] I. Dinur and K. Nissim, "Revealing Information While Preserving Privacy," *Proceedings of the 22nd ACM Symposium on Principles of Database Systems* (*PODS*), San Diego, June 2003, pp. 202-210.

[40] C. Dwork, "Differential Privacy: A Survey of Results," *Proceedings of the 5th International Conference on Theory and Applications of Models of Computation* (*TAMC*), Xi'an, April 2008, pp. 1-19.

[41] A. Blum, K. Ligett and A. Roth, "A Learning Theory Approach to Non-Interactive Database Privacy," *Proceedings of the 40th annual ACM Symposium on Theory of Computing* (*STOC*), Victoria, 2008, pp. 609-618.

[42] X. Xiao and Y. Tao, "Anatomy: Simple and Effective Privacy-Preservation," *Proceedings of the International Conference on Very Large Data Bases* (*VLDB*), Seoul, 2006, pp. 139-150.

[43] N. Maheshwarkar, K. Pathak and V. Chourey, "Privacy Issues for k-Anonymity Model," *International Journal of Engineering Research*, Vol. 1, No. 4, 2011, pp. 1857-1861. doi:10.1109/DBTA.2009.74

[44] X. Hu, Z. Sun, Y. Wu, W. Hu and J. Dong, "k-Anonymity Based on Sensitive Tuples," *First International Workshop on Database Technology and Applications*, Wuhan, 25-26 April 2009, pp. 91-94.

