Proceedings of International Conference
on Mechanical, Electrical and Medical Intelligent System 2017

Extensions of l-diversity to reduce the risk of revealing patient severe health conditions

Osamu Takaki[1, a], Takayuki Asao[2,b] and Yoichi Seki[3,c]

[1]Faculty of Social and Information Science, Gunma University, 4-2 Aramaki-machi, Maebashi, 371-8510, Japan

[2]Big Data Center for Integrative Analysis, Gunma University, 3-39-22 Showa-machi, Maebashi, 371-8511, Japan

[3]School of Science and Technology, Gunma University, 1-5-1 Tenjin-cho, Kiryu, 376-8515, Japan

[a]takaki@gunma-u.ac.jp, [b]asao@gunma-u.ac.jp, [c]seki@cs.gunma-u.ac.jp

Keywords: *k*-anonymity, *l*-diversity, anonymization, medical data, ontology

Abstract. In this paper, l-diversity is extended to reduce the risk of an attacker inferring a patient's severe health conditions based on medical data. The extended versions of l-diversity are defined in accordance with a proposed ontology model by which the severity of a patient's health information is quantified. It is herein shown that the extended l-diversities satisfy the monotonicity property. Additionally, an outline of a process is presented to anonymize medical data. Accordingly, the data satisfy the extended l-diversities and retain the data usability to the greatest extent possible.

1. Introduction

Medical data contain sensitive patient information. Therefore, in many hospitals, when data administrators are requested to provide medical data to users from medical databases for secondary applications, such as data-based research, the administrators should carefully determine the scope and detail level of the provided medical data based on the given purpose and authority of the user. Moreover, at that time, data administrators must decide the anonymization level of the medical data. However, a trade-off exists between the anonymization level of medical data and their usability. It is thus desirable to anonymize the medical data to ensure that it satisfies hospital guidelines and maintains usability of the data to the greatest extent possible.

k-anonymity [1] and l-diversity [2] have been proposed as useful properties in determining the data anonymization level, where k and l denote natural numbers. In what follows, let us consider data to be tables in a relational database, and let T denote a table. A set of attributes in T that can be linked with other tables to identify individuals is called a *quasi-identifier* in T. On the other hand, an attribute in T, the value of which adversaries should be prevented from discovering for individuals in T, is called a *sensitive attribute*. For example, Table 1 contains a quasi-identifier, which consists of "age," "zip code," and "occupation," as well as a sensitive attribute, "disease." T is said to satisfy k-*anonymity* if every record in T is indistinguishable from at least k records with respect to every quasi-identifier in T. For example, Table 1, which has five records, satisfies 2-anonymity. (For

Table 1. Example table with a quasi-identifier consisting of "age", "zip code" and "occupation" as well as with a sensitive attribute "disease"

ID (Dummy)	Age	Zip code	Occupation	Disease
101	50	371-8510	Professor	Parkinson's disease
102	50	371-8510	Professor	Parkinson's disease
103	25	376-8515	Nurse	Bronchitis
104	25	376-8515	Nurse	Gastric ulcer
105	25	376-8515	Nurse	Flu

simplicity, every sensitive attribute is considered not contained in a quasi-identifier.) k-anonymity of T ensures that adversaries are prevented from uniquely linking an individual to a record in T with a quasi-identifier.

However, for an adversary A and a target individual B, even if A cannot uniquely link B to any record, A might link B to a value of a sensitive attribute in *T*. For example, in Table 1, even if A cannot distinguish the records with ID 101 or 102, A will realize that B has Parkinson's disease if A can link B to the two above records. We call this problem a homogeneity attack [2].

To avoid a homogeneity attack, l-diversity has been proposed. Table T is said to satisfy l-*diversity* if every set of records that shares the same values of attributes in a quasi-identifier has at least l different values of every sensitive attribute. For example, Table 1 will satisfy 2-diversity if the value "Parkinson's disease" of the sensitive attribute "disease" in the record with ID 101 is replaced by "myasthenia gravis." However, in the case of medical data where the range of severities of the information described by a sensitive attribute is very broad, a homogeneity attack may not be completely avoided by the use of only l-diversity. For example, from Table 1, in which "Parkinson's disease" in the record with ID 101 is replaced by "myasthenia gravis," attacker *A* may conclude that, although *A* could not uniquely identify the disease of *B* from Table 1, *A* realizes that *B* requires a tremendous expense to fully return to society.

The main purpose of this study was to extend l-diversity to reduce the risk of attackers inferring a patient's severe medical problems based on medical data in the example above. The extended l-diversities are defined based on our proposed ontology model—the Risk-Impact Ontology for Patients' Sensitive Information (RIOPSI)—which enables quantification of the severities of a patient's health information. In this paper, it is shown that the extended l-diversities satisfy the monotonicity property. In addition, an outline of a process is presented to anonymize medical data. Accordingly, the data satisfy the extended l-diversities and maintain the usability of the data to the greatest extent possible by using the monotonicity property of the extended l-diversities.

2. Modeling of Patient Medical Condition Severity

This section explains concepts in RIOPSI to define the severity of a patient's health condition. An approach to quantifying the severity of the information based on RIOPSI is also described.

2.1 Risk-Impact Ontology for Patients' Sensitive Information

RIOPSI is described by $\mathbb{O}$ and mainly consists of (i) an attacker's objectives and (ii) a patient's health conditions and severity criteria. Severity criteria are represented as sets of especially severe patient conditions that are classified by types of patient medical conditions. The main concepts in $\mathbb{O}$ are outlined below.

According to psychological studies on cyber attacks [3, 4] and insider threats [5, 6], attacker motivations are classified into the following types: (1) Emotional motivation: (1.1) Pleasure, (1.2) curiosity, (1.3) revenge, (1.4) revelation, and (1.5) destruction. (2) Commercial motivation: (2.1) Data sales, (2.2) business operations, and (2.3) intimidation. Let us apply the motivations above to the case of a homogeneity attack. Then, the adversary's main objectives in accessing patient conditions are classified into the following problems.

I. Problems that directly inflict major damage on patients only by being known by others.
II. Problems that patients are eager to solve, even if the cost is immense.

We divide these two problem types into several categories and consider the relevant attributes in the tables, which are stored in most hospital databases. Moreover, we consider the severity criteria of the categorized conditions by defining sets of especially severe information as values of the related attributes. The results are given in Table 2.

Table 2. Classification of Sensitive Information, Related Attributes, and Their Special Values

Large Class of Sensitive information	Middle Class of Sensitive information	Small Class of Sensitive information	Related Attributes (Underlined Part) and Sets of Special Values of the Attributes
1. information that inflicts significant damage on patients directly only by being known by others.	1.1. information that inflicts significant damage not only on patients but also on their offsprings	1.1.1. information about diseases of genes	For the attribute "disease," we consider the set of values that are assigned as diseases of genes by the administration of health.
	1.2. information that inflicts significant disadvantages on patients institutionally	1.2.1. information about diseases assigned as intractable diseases	For "disease," we consider the set of values that are assigned as intractable diseases by the administration of health.
	1.3. information that inflicts significant damage on patients' human rights	1.3.1. information about significant psychiatric disorders	For "disease," we consider the set of values that specialists such as doctors of psychiatric diseases select as significant psychiatric disorders.
2. Otherwise than the above	2.1. Information about patients' life spans	2.1.1. information about diseases that have a major impact on patients' life spans	For "disease," we consider the set of values whose survival rate (for example, 5-year survival rates) are low (for example, less than 30%).
		2.1.2. information about patients' outcomes	For the pair of "disease" and its "medical treatment" including operations, we consider the set of pairs of values whose survival rates after the medical treatments are low.
	2.2. Information about patients' quality of life (QOL)	2.2.1 and 2.2.2. information about financial burdens of patients	For "disease," we consider the set of values that the institution of expensive medical treatments can be applied to. (In the case of Japan, one can define 2-stage sets according to the criteria defined by the health ministry.)
			For "treatment" or "medicines," we consider the set of values that are assigned as expensive medical treatments by the administration of health.
		2.2.3, 2.2.4 and 2.2.5. information about degrees of disability to patients' social and/or personal life	For "disease," we consider the set of values that specialists select as diseases by which patients have difficulty to get back into society.
			For "disease," we consider the set of values that specialists select as diseases by which patients have difficulty to have their daily life.
			For attributes about durations of hospital stays, we consider the set of (tuples of) values that indicate that the patients are hospitalized for long periods. (For example, one can define 3-stage sets by more than 60 days-, more than 120 days- and more than 180 days-hospitalization.)
	2.3. information that inflict damage on patients' human rights (other than the middle class 1.3)	2.3.1. information by which others might have prejudice toward patients' life styles	For "disease," we consider the set of values that specialists select as diseases by which others might have prejudice toward patients' life styles.
		2.3.2. information by which others might have prejudice toward patients' appearances	For "disease," we consider the set of values that specialists select as diseases by which others might have prejudice toward patients' appearances.

Each set of special values that is defined in the right-most column of Table 2 is called a *special values set*.

Remark 1. A survival rate, such as a five-year survival rate, is determined based on not only the disease, but also the disease degree of progression. However, for simplicity, we regard a value of the attribute "disease" as a disease with its degree of progression.

Remark 2. In what follows, we regard every pair (and every tuple) of sensitive attributes in the small class (2.1.2) (and (2.2.5), respectively) as a single sensitive attribute. Moreover, for a pair (d, t) of a disease, d, and a medical treatment, t, which is defined in the small class (2.1.2), if d is contained in a special values set S, then we regard (d, t) as contained in S.

2.2 Quantification of Patient Condition Severity Based on $\mathbb{O}$

In this section, we quantify the severities of values and records in medical database tables from adversaries' viewpoints. In Definition 1, we define a "severity number" $\mathrm{s}(v)$ of a value, v, by which we describe the severity of v, so that it satisfies the following principles.

i. For values v and u, if v is contained in a special values set in the first large class of sensitive information, but u is not, then $\mathrm{s}(u) < \mathrm{s}(v)$.
ii. For values v and u in the first large class, if $\mathbb{G}_u \subsetneqq \mathbb{G}_v$, then $\mathrm{s}(u) < \mathrm{s}(v)$, where $\mathbb{G}_u$ and $\mathbb{G}_v$ are the set of special values sets in the first large class that contains u and v, respectively.
iii. For values v and u that are not in the first large class, but are in the second large class, if v and u are contained in special values sets in different middle classes, then the severities of v and u are not comparable.
iv. However, if the severities of v and u above are compared from the specified viewpoint represented by the middle class (2.1), (2.2), or (2.3) in Table 2, and if $\mathbb{G}_u \subsetneqq \mathbb{G}_v$, then $\mathrm{s}(u) < \mathrm{s}(v)$, where $\mathbb{G}_u$ and $\mathbb{G}_v$ are the set of special values sets in the same middle class (2.1), (2.2), or (2.3) as well as $\mathbb{G}_u$ and $\mathbb{G}_v$ contain u and v, respectively.

We believe that the above principles (i) and (ii) are reasonable. Note that the severity of a patient's information from an adversary's viewpoint differs from the patient's severity itself. We also consider the principles (iii) and (iv), because it is not easy to compare the severities of patients' informations if they are considered from different viewpoints that are represented by the middle classes (2.1), (2.2), and (2.3) in Table 2. Therefore, we define the severity number of v according to not only the large class type of, but also the middle class type.

Definition 1. (1) Let m be the number of the middle classes with item number $(2.m)$ in Table 2, which we call the *middle class type*. Then, we define *severity number* $s_m(v)$ of value v with respect to m as follows.

1. If v is contained in a special values set in the first large class, then $s_m(v)$ is defined independently of m to be $n + N$. Here, n denotes the number of special values sets in the first large class that contain v, and N denotes the maximum number in the set of all severity numbers satisfying condition (2) below.
2. If v is contained in no special values set in the first large class, then $s_m(v) = n$. Here, n denotes the number of special values sets in the middle class with type m that contain v.

(2) For record λ in a table and middle class type m, severity number $s_m(\lambda)$ of λ with respect to m is the maximum number of $s_m(v)$ of all values v in λ.

3. $\mathbb{O}$-Based l-Diversity

In this section, we extend l-diversity based on $\mathbb{O}$ and the severity numbers defined in Section 2. Let T be a table, λ a record in T, π a quasi-identifier in T, and q a tuple of values of π in λ. Then, the set of records in T that share q as the tuple of the values of π is called the π-*block* of q.

Definition 2. Let l be a natural number and m be a middle class type. Then, a π-block Λ is said to satisfy $\mathbb{O}(m)$-*l-diversity* if, for every sensitive attribute σ, there exists at least l values $v_1, \dots, v_l$ of σ in Λ with severity numbers $s_m(v_1), \dots, s_m(v_l)$ that differ from each other. Moreover, Λ is said to satisfy $\mathbb{O}$-*l-diversity* if Λ satisfies $\mathbb{O}(m)$-l-diversity for all types m of middle classes. Furthermore, T is said to satisfy $\mathbb{O}(m)$-*l-diversity* (or $\mathbb{O}$-*l-diversity*) if all blocks in T satisfy $\mathbb{O}(m)$-l-diversity (or $\mathbb{O}$-l-diversity, respectively).

For table T, if T satisfies $\mathbb{O}(m)$-l-diversity for some type m, then it clearly satisfies l-diversity. Moreover, one can easily extend other l-diversity types defined in [2] by replacing the differences of values by those of the severity numbers of the values.

Severity numbers of most values would be very low. Thus, the conditions of $\mathbb{O}(m)$-l-diversity and $\mathbb{O}$-l-diversity in Definition 2 may be too strict. If it is not necessary to focus on records with a low severity number, Definition 3 would be more useful.

Definition 3. Let l be a natural number and m a middle class type. Then, π-block Λ is said to satisfy *downward*-$\mathbb{O}(m)$-*l-diversity* if there exists a record, λ, in Λ that satisfies $s_m(\lambda) \leq N - l$, where N is the maximum number of all severity numbers. Moreover, Λ is said to satisfy *downward*-$\mathbb{O}$-*l-diversity* if Λ satisfies downward-$\mathbb{O}(m)$-l-diversity for all types m of middle classes. Furthermore, T is said to satisfy *downward*-$\mathbb{O}(m)$-*l-diversity* (or *downward*-$\mathbb{O}$-*l-diversity*) if all block Λ in T satisfy downward-$\mathbb{O}(m)$-l-diversity (or downward-$\mathbb{O}$-l-diversity, respectively).

Note that N in Definition 3 is independently determined of table T and that the downward version of $\mathbb{O}(m)$-l-diversity has no logical strength relationship with l-diversity. Actually, if T has no value with a severity number $> N - l$, then T automatically satisfies *downward*-$\mathbb{O}$-*l-diversity*.

4. Generalization of Medical Data Based on $\mathbb{O}$-Based l-Diversity

In this section, we outline a process to anonymize medical data based on extended l-diversities defined in Definitions 2 and 3, which we call $\mathbb{O}$-*based* l-*diversities*. To this end, we first show monotonicity of $\mathbb{O}$-based l-diversities. For simplicity, in what follows, for a table, T, we consider that all quasi-identifiers in T are integrated and that T has only one quasi-identifier.

Let T be a table that consists of the (integrated) quasi-identifier π and a sensitive attribute σ. In addition, λ denotes a record in T, and q represents a tuple of values of π in λ. Moreover, let Q be the domain of π, and let Q^* be a set $\{Q_1, \dots, Q_n\}$ of subsets of Q that satisfies $\mathrm{Q} = Q_1 \cup \cdots \cup Q_n$ and $Q_i \cap Q_j = \emptyset$ for each $i, j \leq n$ with $i \neq j$. Furthermore, T^* denotes a table that consists of the quasi-identifier π^* and the sensitive attribute σ, where π^* has Q^* as its domain. Then, T^* is called a *generalization* of T if T and T^* share the same number I of their records and if, for every $i \leq I$, $q_i \in q_i^*$ and $s_i = s_i^*$, where q_i and q_i^* denote the values of π and π^* in the i-th records of T and T^*, respectively, and s_i and s_i^* denote the values of σ and σ^* in the i-th records of T and T^*, respectively.

For tables T and T^* above, let i be a number with $i \leq I$, Λ be the π-block in T of q_i, and Λ^* be the π^*-block in T^* of q_i^*. Then, for every $j \leq I$, if the j-th record λ_j of T is contained in Λ, then the j-th record λ_j^* of T^* is contained in Λ^* and the value s_j of σ in λ_j is the same as the value s_j^* of σ^* in λ_j^*. Thus, by the conditions of Definitions 2 and 3, one can easily demonstrate Proposition 1.

Proposition 1. All $\mathbb{O}$-based l-diversities satisfy the monotonicity property. For example, if table T satisfies $\mathbb{O}(m)$-l-diversity for a type m, then every generalization T^* also satisfies $\mathbb{O}(m)$-l-diversity. The same holds for other type $\mathbb{O}$-based l-diversities.

The monotonicity property of $\mathbb{O}$-based l-diversities implies that one can easily apply to $\mathbb{O}$-based l-diversities the algorithm "Incognito" [7], which has been employed for data generalization to satisfy k-anonymity and l-diversity (see also [2]). As an application, we outline a process to generalize

medical data (tables) to satisfy an $\mathbb{O}$-based l-diversity maintaining the data usability to the greatest possible extent by using Incognito as follows.

i. In advance of generalization of medical data, experts of medical informatics, administrators of medical databases, and hospital research ethics committees collaborate in formulating a guideline for appropriate use of medical data for research purposes in the hospital.

ii. Administrators of medical databases and users (researchers) of medical data collaborate in deciding the scope of data T that the users desire as well as the conditions and priority for generalization of the (integrated) quasi-identifier q in T based on the guideline above. Then, for domain Q of q, a sequence $\mathbb{Q} = \{Q, Q^*, Q^{**}, \ldots, Q^{*\cdots*}\}$ of iteration results of generalizations of Q is specified, which we call a *strategy of generalization* of T.

iii. Based on the guideline in (i) and the discussion in (ii), one of the $\mathbb{O}$-based l-diversities $\mathbb{D}$, including parameters, is determined and Incognito is adjusted based on $\mathbb{D}$.

iv. By applying strategy $\mathbb{Q}$ to $\mathbb{D}$-adjusted Incognito, the user can obtain generalized data T^* that satisfy $\mathbb{D}$ by the minimum iterations of generalizations according to strategy $\mathbb{Q}$.

5. Conclusion

In this paper, we proposed several extensions of l-diversity to reduce the risk of attacker inference of severe patient medical conditions based on medical data. To this end, we defined the RIOPSI ontology model and quantified the severities of a patient's health information based on RIOPSI. Moreover, we showed that our extended versions of l-diversity satisfy the monotonicity property. We hence outlined a process to generalize medical data (tables) to satisfy the extended l-diversities maintaining of data usability to the greatest extent possible by using the adjusted Incognito algorithm.

With respect to improvements, in Table 2, it would be more effective to define more refined subsets of the several special values sets. For example, it would be better to define subsets of the special values set defined in the small class (2.1.1) by using a one-year survival rate and/or a three-year survival rate. An approach to creating more refined subsets remains for future work.

References

[1] L. Sweeney, "k-anonymity: a model for protecting privacy", ***Int. J. Uncertain. Fuzziness Knowl.-Based Syst***. Vol. 10, No. 5, 2002, pp. 557-570.

[2] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "L-diversity: Privacy beyond k-anonymity", ***TKDD*** Vol. 1, No. 1(3), 2007, pp. 1-52.

[3] C. A. Meyers, C A, S. S. Powers, D. M. Faissol, "Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches", ***Technical Report in Lawrence Livermore National Laboratory (LLNL), Livermore***, CA: LLNL-TR-419041, DOI: 10.2172/967712, 2009.

[4] S. Atkinson, "Psychology and the hacker: Psychological incident handling", White Paper, SANS Institute, 2015.

[5] D. Cappelli, A. G. Desai, A. P. Moore, T. J. Shimeall, E. A. Weaver, B. J. Willke, "Management and education of the risk of insider threat (MERIT): system dynamics modeling of a computer system", White Paper, Carnegie Mellon University, 2008.

[6] "Report on measure against human threats to information security", White Paper, The Nikkoso Research Foundation for Safe Society, 2010 (in Japanese).

[7] K. LeFevre, D. J. DeWitt, and R. Ramakrishnan. "Incognito: efficient full-domain K-anonymity", ***In Proceedings of the 2005 ACM SIGMOD International Conference on Management of Data (SIGMOD '05)***. ACM, New York, NY, USA, 2005, pp. 49-60.