JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 28 No. 9, pp. 81-92, September 2023
https://doi.org/10.9708/jksci.2023.28.09.081

Privacy Model Recommendation System Based on Data Feature Analysis

Seung Hwan Ryu*, Yongki Hong*, Gihyuk Ko*, Heedong Yang*, Jong Wan Kim**

*Principal Researcher, Cyber Security Research Center, KAIST, Daejeon, Korea
*Researcher, Cyber Security Research Center, KAIST, Daejeon, Korea
*Researcher, Cyber Security Research Center, KAIST, Daejeon, Korea
*Researcher, Cyber Security Research Center, KAIST, Daejeon, Korea
**Assistant Professor, Software Convergence Education Center, Sahmyook University, Seoul, Korea

[Abstract]

A privacy model is a technique that quantitatively restricts the possibility and degree of privacy breaches through privacy attacks. Representative models include *k*-anonymity, *l*-diversity, *t*-closeness, and differential privacy. While many privacy models have been studied, research on selecting the most suitable model for a given dataset has been relatively limited. In this study, we develop a system for recommending the suitable privacy model to prevent privacy breaches. To achieve this, we analyze the data features that need to be considered when selecting a model, such as data type, distribution, frequency, and range. Based on privacy model background knowledge that includes information about the relationships between data features and models, we recommend the most appropriate model. Finally, we validate the feasibility and usefulness by implementing a recommendation prototype system.

▸ **Key words**: Privacy model, Data Privacy, De-identification, Background knowledge, Data feature analysis, Recommendation

[요 약]

프라이버시 모델이란 프라이버시 공격을 통한 개인정보의 유출 가능성과 위험 정도를 정량적으로 제한하는 기법이다. 대표적인 모델로 *k*-익명성, *l*-다양성, *t*-근접성, 차분 프라이버시 등이 있다. 지금까지 많은 프라이버시 모델들이 연구되어 왔지만, 주어진 데이터에 대해 가장 적합한 모델을 선택하는 문제에 대한 연구는 미흡하다. 본 연구에서는 개인정보 유출 문제를 막기 위한 최적의 프라이버시 모델 추천 시스템을 개발한다. 본 논문에서는 프라이버시 모델 선택 시 고려해야 할 데이터 특성(예: 데이터 타입, 분포, 빈도, 범위 등)을 분석하고 데이터 특성과 모델 간의 연관관계 정보를 포함하는 프라이버시 모델 배경지식에 기반한 최적 모델을 추천한다. 마지막으로 타당성과 유용성을 검증하기 위해 추천 프로토타입 시스템을 구현하였다.

▸ **주제어**: 프라이버시 모델, 데이터 프라이버시, 비식별화, 배경지식, 데이터 특성 분석, 추천

• First Author: Seung Hwan Ryu, Corresponding Author: Seung Hwan Ryu
*Seung Hwan Ryu (deepryu@kaist.ac.kr), Cyber Security Research Center, KAIST
*Yongki Hong (ykhong@kaist.ac.kr), Cyber Security Research Center, KAIST
*Gihyuk Ko (gihyuk.ko@kaist.ac.kr), Cyber Security Research Center, KAIST
*Heedong Yang (heedong@kaist.ac.kr), Cyber Security Research Center, KAIST
**Jong Wan Kim (kimj@syu.ac.kr), Software Convergence Education Center, Sahmyook University
• Received: 2023. 07. 20, Revised: 2023. 08. 24, Accepted: 2023. 09. 04.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

데이터는 디지털 경제에서 기업에게 귀중한 자산이며, 의료 및 인구 통계 연구, 시장 분석, 인공지능 학습 등 다양한 목적으로 공유 및 배포되어 활용되고 있다[1,2]. 데이터에는 종종 개인에 대한 건강 정보, 금융 거래, 소셜 네트워크 활등 등의 개인정보가 포함될 수 있다[3]. 하지만 데이터를 공유하고 배포하는 과정에서 데이터가 올바르게 처리 및 가공되지 않는다면 데이터에 내포된 개인정보가 유출되거나 적대적 의도를 가진 공격자가 개인정보를 유추하는 등 프라이버시 유출 문제가 발생할 수 있다. 예를 들어, 방대한 양의 사용자 데이터를 수집하여 학습한 국내 챗봇 서비스에서 데이터에 포함된 개인의 계좌번호, 전화번호나 주소 등의 개인정보가 유출된 바 있다[4].

데이터 활용 시 개인정보 유출의 위험은 데이터 비식별화를 통해 극복할 수 있다[5]. 비식별화는 개인정보의 일부 또는 전부를 삭제하거나 변경하여 특정 개인을 식별할 수 없도록 하는 조치이다. 비식별화의 동의어로서 익명화라는 용어가 자주 사용된다[6]. 데이터의 비식별화를 위해서는 속성(Attribute)의 특징과 중요도에 따라 식별자(ID: Identifier), 준식별자(QI: Quasi-Identifier), 그리고 민감속성(SA: Sensitive Attribute)으로 분류하는 작업이 선행되어야 한다.

Table 1. Example patient table

ID	QI		SA
Name	Age	Zipcode	Disease
Alice	21	12021	Diabetes
Bob	25	12021	Diabetes
Cathy	25	12082	Diabetes
Daniel	41	13001	Flu
Emily	49	13002	Asthma
Fred	47	13007	Diabetes
Gladys	31	12023	Asthma
Henry	32	12082	Flu
Irene	38	12089	HIV

식별자는 이름, 주민등록번호, 전화번호 등과 같이 개인을 바로 식별할 수 있는 정보를 가진 속성을 말하며 비식별화 과정에서 삭제되어야 한다. 준식별자는 나이, 성별, 우편번호 등과 같이 속성값 하나만으로 특정 개인을 식별하기 어렵지만, 여러 가지 다른 준식별자를 조합하여 식별 가능성을 높일 수 있는 속성이다. 민감속성은 개인의 급여, 병명, 계좌잔고와 같이 민감한 정보를 포함하는 속성이며 비식별화를 통해 보호받아야 하는 속성이다. 예를 들어, Table 1의 질병 테이블에서 식별자는 이름, 준식별자는 나이, 우편번호이고 민감속성은 질병명이다.

데이터를 비식별화하기 위해 많은 프라이버시 모델들이 연구되어 왔다[7,8]. 프라이버시 모델이란 프라이버시 공격을 통한 원본 정보의 유출 가능성과 위험 정도를 정량적으로 제한하는 기법이다. 대표적으로 k-익명성(k-anonymity)[9], l-다양성(l-diversity)[10], t-근접성(t-closeness)[11], 차분 프라이버시[12] 등이 있다. 그동안 비식별화 관련 많은 연구가 이루어져왔지만, 주어진 데이터에 대해 적합한 프라이버시 모델을 선택하는 문제는 그 중요성에도 불구하고 연구는 거의 이루어지지 않았다. 본 논문에서는 이러한 문제를 해결하기 위해 주어진 데이터에 최적의 프라이버시 모델을 추천하는 시스템을 개발한다. 이를 위해, 우선 주어진 데이터의 특성을 분석한 후, 데이터 특성과 모델 간의 연관관계 정보를 표현하는 프라이버시 모델 배경지식(Privacy Model Background Knowledge)에 기반하여 최적의 프라이버시 모델을 추천한다.

본 논문의 구성은 다음과 같다. 2장에서는 프라이버시 공격 유형, 프라이버시 모델, 익명화 연산, 그리고 관련 연구를 논의한다. 3장에서는 데이터 특성 분석과 프라이버시 모델 배경지식에 기반한 모델 추천 알고리즘, 시스템 구현, 그리고 성능평가 결과를 논의한다. 마지막으로 결론 및 향후 연구 과제는 4장에서 서술한다.

II. Preliminaries

1. Motivating Example

k-익명성은 개인 식별 노출 위험을 예방하기 위한 가장 널리 사용되는 모델 중 하나이다[13,14]. 이 모델은 주어진 테이블을 중복되지 않는 레코드 그룹으로 분할하고, 각 그룹에는 적어도 k개의 동일한 준식별자 값을 가진 레코드들이 존재하게 한다. 이러한 레코드 그룹을 동질 클래스(EC: Equivalence Class)라고 한다. 예를 들어, Table 2는 3-익명성을 만족하도록 Table 1을 비식별화한 테이블이다. 이 경우, 공격자가 공격 대상의 준식별자값을 알고 있다고 가정했을 때, Table 1의 경우 특정 레코드를 바로 식별할 수 있지만, Table 2의 경우에는, 식별할 확률이 1/3로 줄어든다.

위의 3-익명화된 테이블 예제에서 동질 클래스 EC_1의 민감 속성값은 모두 Diabetes이므로, 공격하고자 하는 대상의 준식별자값이 EC_1에 속한 경우, 그 대상의 민감 속성값이 Diabetes라는 것을 바로 유추할 수 있다. 이러한 공

격을 동질성 공격(Homogeneity Attack)이라 한다[10]. *l*-다양성은 이러한 동질성 공격을 방어하는데 효과적인 모델이며 비식별화된 테이블에서 각각의 동질 클래스가 최소 *l*개의 민감 속성값을 가지도록 한다. 예를 들어 Table 3의 경우, 동질 클래스 EC_1의 민감 속성값의 종류가 Diabetes, Asthma 2개, EC_2의 경우에는 Flu, Asthma, Diabetes 3개, EC_3는 Diabetes, Flu, HIV 3개를 가짐으로 Table 3은 2-다양성을 만족한다.

Table 2. 3-anonymous table

EC	QI		SA
	Age	Zipcode	Disease
EC_1	[20,30)	120**	Diabetes
	[20,30)	120**	Diabetes
	[20,30)	120**	Diabetes
EC_2	[40,50)	130**	Flu
	[40,50)	130**	Asthma
	[40,50)	130**	Diabetes
EC_3	[30,40)	120**	Asthma
	[30,40)	120**	Flu
	[30,40)	120**	HIV

Data utility: DM(27= 9+9+9)
Privacy level: less protective

Table 3. 2-diverse table

EC	QI		SA
	Age	Zipcode	Disease
EC_1	[20,40)	1202*	Diabetes
	[20,40)	1202*	Diabetes
	[20,40)	1202*	Asthma
EC_2	[40,50)	1300*	Flu
	[40,50)	1300*	Asthma
	[40,50)	1300*	Diabetes
EC_3	[20,40)	1208*	Diabetes
	[20,40)	1208*	Flu
	[20,40)	1208*	HIV

Data utility: DM(27= 9+9+9)
Privacy level: more protective

위의 k-익명성과 l-다양성 예제에서, 두 모델은 분별력 척도(DM: Discernibility Metric)[7,10]로 계산한 데이터 유용성 측면에서는 동일한 결과를 나타내지만, 프라이버시 보호 측면에서는 l-다양성이 k-익명성 보다는 더 효과적이라는 것을 알 수 있다. 왜냐하면 l-다양성 모델은 레코드 그룹 내에서 민감한 속성 값의 다양성을 유지함으로써 개인정보 유출의 가능성을 줄일 수 있기 때문이다. 따라서, 주어진 데이터셋에 가장 적합한 모델을 선택하는 것은 데이터의 프라이버시를 보호함과 동시에 데이터의 유용성을 보존하는데 있어서 중요하다.

2. Privacy Attack

프라이버시 공격은 공격자가 특정 개인을 식별하거나 개인의 민감 속성을 유추하기 위해 자신이 가지고 있는 배경지식(Background Knowledge)을 이용할 때 발생한다. 이러한 공격은 레코드 연계(Record Linkage), 속성 연계(Attribute Linkage), 테이블 연계 (Table Linkage), 그리고 확률 공격(Probabilistic Attack)으로 나눌 수 있다[7,15].

Record Linkage. 레코드 연계는 공격자가 공격하고자 하는 대상의 준식별자 속성값을 알고 있다고 가정했을 때, 그 속성값을 가지고 임의의 레코드가 누구를 의미하는지 알아내는 공격이다. 예를 들어, Table 1에서 공격자가 Alice는 우편번호 12021에 거주하고 25세 미만임을 알고 있다면, 공격자는 공격 대상이 첫 번째 레코드에 속한다는 것을 유추할 수 있다.

Attribute Linkage. 이 공격은 배포된 테이블을 통해 공격 대상의 민감 속성값을 추론하는 공격이다. 배포된 테이블이 레코드 연계 공격을 효과적으로 방어한다고 해도 속성 연계는 이루어질 수 있다. 예를 들어, Table 1에서 공격자가 Cathy가 25세라는 사실만을 알고 있다면, 공격자는 Cathy의 레코드를 정확히 식별할 수는 없지만, 그녀가 Diabetes에 걸렸다는 것을 유추할 수 있다.

Table Linkage. 이 공격은 배포된 테이블을 통해 공격 대상의 유무를 유추하는 공격이다. 위의 레코드 연계와 속성 연계는 공격자가 공격하고자 하는 대상이 테이블에 포함되어 있다는 것을 안다고 가정하지만, 테이블 연계는 공격 대상 존재의 유무 자체에 초점을 맞춘다. 예를 들어, 암 환자를 포함한 데이터셋이 공개되면, 단순히 데이터셋에 개인이 포함되어 있는지 여부를 판단하는 것만으로도 상당히 민감한 정보가 노출될 우려가 있다.

Probabilistic Attack. 이 공격은 공격자가 배포된 테이블을 보기 전의 정보와 본 후의 정보의 차이가 클 경우 그 차이를 이용해 정보를 추론하는 공격이다. 이러한 공격을 완화하기 위해서는 데이터 배포자가 이 차이를 최소화해야 한다[7].

3. Privacy Model

프라이버시 공격을 막기 위해 연구된 프라이버시 모델들은 신택틱(Syntactic) 모델과 시맨틱(Semantic) 모델로 분류될 수 있다[16]. 신택틱 모델은 프라이버시 보호을 위해 동질 클래스 내에서 동일한 준식별자값을 갖는 최소의 레코드 수, 민감 속성값의 빈도 등과 같이 데이터의 구조나 특성에 관한 조건을 충족시키는데 중점을 둔 모델이다. 가

장 널리 알려진 신택틱 모델은 레코드 연계 공격에 대응하는 k-익명성 모델이다. 하지만 이 모델은 속성 연계 혹은 테이블 연계 공격 등에 대응하지 못하는 문제가 있다. 이러한 문제에 대응하기 위해 l-다양성, t-근접성, β-유사도(β-likeness) 등과 같은 모델들이 제안되었다. 시맨틱 모델은 데이터의 구조나 특성에 관여하는 대신 데이터의 의미나 문맥을 고려한다. 예를 들어, ϵ-차분 프라이버시[12]는 원본 테이블 T_1에 교란 메커니즘 F를 적용한 결과 A와 T_1에서 데이터를 하나 추가한 테이블 T_2에 교란 메커니즘 F를 적용한 결과 B가 서로 구별 불가능하도록 만드는 모델이다. 여기서 교란 메커니즘 F는 값에 노이즈를 추가하는 방식이 주로 사용되며, 이러한 추가되는 노이즈는 일반적으로 Laplace, Gaussian, Exponential 분포 등을 따른다.

4. Anonymization Operations

익명화 연산은 원본 데이터를 배포하기 전에 데이터를 변형하기 위해 사용된다. 이러한 연산에는 일반화(Generalization), 삭제(Suppression), 해부화(Anatomization), 순열(Permutation), 교란(Perturbation) 등이 포함된다[7]. 일반화는 특정 값을 계층 트리(Hierarchy Tree)에 따라 더 일반적인 값으로 대체하는 방법이다. 예를 들어, 나이 25세를 나이 구간 [20,30]으로 일반화할 수 있다. 삭제는 데이터 값을 삭제하거나 “*”, “#”와 같은 특수 문자로 대체하는 방법이다. 해부화는 준식별자와 민감 속성 간의 관계를 분리하며, 순열은 동질 클래스 내에서 민감 속성값을 섞고(shuffling), 교란은 통계적 특성을 유지하면서 데이터에 노이즈를 추가하거나 값들을 교환하거나 합성 데이터를 생성하는 방법이다.

5. Related Work

2010년 Fung 등[7]은 프라이버시 공격 유형을 설명하고 이러한 공격에 대응할 수 있는 프라이버시 모델, 익명화 연산, 프라이버시 보호와 데이터 유용성을 계산하기 위한 척도 등을 정리하였다. Majeed 등[8]은 프라이버시 모델을 설명하고 이들의 장단점 그리고 모델들을 적용할 수 있는 데이터 유형 등을 기술하였다. Cuncha 등[17]은 데이터의 유형에 따른 비식별화 기술들에 대해 정리하였으며, 정형 데이터, 반정형 데이터, 그리고 비정형 데이터에 대한 비식별화 기술들에 대해 소개하였다. 하지만 이러한 조사 논문에 따르면 데이터 특성에 따라 최적의 프라이버시 모델을 선택하는 문제에 대한 연구가 미흡하다[17]. 2019년에 과학기술정보통신부에서 발간한 개인정보 비식별 기술 가이드라인[18]에서는 비식별화 기술 적용 시 검토사항, 개인정보 속성 결정 방법, 비식별화 기술의 종류 등을 설명하였으며 비식별화된 결과의 적정성 평가를 위해 k-익명성, l-다양성, t-근접성을 사용할 것을 제안하였다. Psaraftis 등[19]는 개인정보를 효과적으로 보호하고 또한 정보 손실을 최소화하기 위한 최적의 프라이버시 모델을 선택하기 위한 시스템을 개발하였다. 이 논문에서 제안하는 시스템은 사용자들이 자신의 데이터와 개인정보 보호 요구사항을 입력하면, 해당 데이터에 가장 적합한 프라이버시 모델을 추천해주는 기능을 가지고 있다. 이를 위해 미리 정의된 사용자 요구사항들을 의사결정 트리(decision tree)로 구성하였으며 이러한 트리에서 중간 노드는 사용자 요구사항에 해당되며 단말 노드는 추천될 프라이버시 모델을 나타낸다. 저자들은 제안된 추천 시스템의 구체적인 동작 방식과 구현 방법에 대해 설명하였다. 하지만 프라이버시 모델 관련 질문에 대한 사용자 답변에 기반하여 프라이버시 모델을 추천하는 [19] 연구와는 다르게 본 논문에서는 주어진 데이터셋의 특성을 분석한 후 데이터 특성과 모델 간의 연관관계 정보를 포함하는 프라이버시 모델 배경지식에 기반하여 프라이버시 모델을 추천한다.

III. The Proposed Scheme

1. Overall Process

제안된 비식별화 프로세스는 Fig. 1에 나와 있는 것과 같이 세 단계로 구성된다.

Fig. 1. Overall Process

Data Feature Analysis. 이 단계에서 데이터 배포자는 원본 데이터 D에서 식별자를 제거하고, 준식별자와 민감 속성을 선택한다. 그런 다음, 선택된 준식별자 혹은 민감 속성값에 대해 데이터 특성(예: 데이터 타입, 분포, 범위 등)을 분석한다.

Model Recommendation. 이 단계에서는 식별된 데이터 특성에 기반하여 적절한 프라이버시 모델이 추천된다. 모델 추천을 위해 데이터 특성과 모델 간의 연관관계 정보를 포함하는 프라이버시 모델 배경지식을 이용한다.

Data De-identification. 이 단계에서는 추천된 프라이버시 모델을 사용하여 주어진 원본 데이터 D를 비식별화한다. 본 연구에서 개발된 프로토타입은 GUI를 통해 추천

된 모델의 매개변수(예: *k*-익명성의 k, *l*-다양성의 l)를 설정할 수 있도록 지원한다.

2. Data Feature Analysis

본 절에서는 적절한 프라이버시 모델을 선택하는데 고려될 수 있는 데이터 특성에 대해 설명한 후, 이러한 특성을 식별하는 방법에 대해 논의한다. 데이터 특성이란 데이터의 고유한 속성 또는 특징을 나타내는 것을 의미하며 데이터의 종류와 구성 요소에 따라 다양하게 나타날 수 있다. 예를 들어, 이러한 특성에는 데이터 타입, 범주형 또는 수치형 값의 여부, 데이터 값들의 분포, 빈도, 범위 등이 포함될 수 있다. 데이터 특성은 특성 분석 연산자(III.3 절)를 사용하여 식별된다. 식별된 데이터 특성은 주어진 데이터에 가장 적합한 프라이버시 모델을 선택하는 데 중요한 역할을 한다. 이러한 데이터 특성을 분석하는 것은 일회적인 과정이 아니라 특성 분석이 진행됨에 따라 데이터와 관련이 있는 새로운 특성이 발견되거나, 이전에 식별된 특성이 기대했던 만큼 유용하지 않은 경우도 있을 수 있다.

본 논문에서는 F를 데이터 특성 $f_1,f_2,...,f_n$의 집합으로 가정한다. Table 4는 몇몇 샘플 데이터 특성들을 보여준다. 데이터 분석을 위해 속성 A_i가 주어지면, A_i의 값들은 동질 클래스에 따라 여러 그룹으로 나누어질 수 있다. 우리는 이러한 그룹을 속성 그룹 (AG, Attribute Group)이라고 하고 AG_{A_i}로 표기한다. 예를 들어, Table 5는 Table 1의 원본 테이블을 일반화하여 변형한 테이블이다. 이 테이블에서 질병 속성의 값들은 세 개의 속성 그룹으로 나누어진다: $AG^{1_{disease}}, AG^2_{disease}, AG^3_{disease}$. 일부 속성 그룹은 한 개 이상의 특성을 가질 수 있다. 어떠한 특성을 갖는 속성 그룹을 특성 속성 그룹 (Feature Attribute Group, FAG)이라고 하고 $FAG^{F'}_{A_i}$로 표기한다: 즉, 특성 $F' \subseteq F$를 가지는 속성 Ai의 값들의 그룹이다. 예를 들어, Table 5에서 특성 속성 그룹 $FAG^{sameValue}_{disease}$은 특성 "sameValue"를 가진 속성 값들의 집합이다.

Table 4. Sample features

Feature	Description
sameValue	If attribute group AG_i has the same values, YES; else No.
similarValue	If attribute group AG_i has similar values, YES; else No.
different Sensitivity	If attribute group AG_i has different sensitivity level of values, YES; else No.
skewness	If attribute group AG_i has skewed values, YES; else No.
duplicate Record	If equivalence class EC_i has duplicate records, YES; else No.

Table 5. Feature Analysis

EC	SA Disease	AG	Feature	FAG
EC_1	Diabetes Diabetes Diabetes	$AG^1_{disease}$	sameValue	$FAG^{sameValue}_{disease}$
EC_2	Flu Asthma Diabetes	$AG^2_{disease}$	-	-
EC_3	Asthma Flu HIV	$AG^3_{disease}$	different Sensitivity	$FAG^{differentSensitivity}_{disease}$

3. Feature Analysis Operators

데이터 배포자는 특성 분석 연산자(이하 분석 연산자)를 사용하여 데이터 값에서 특성을 식별할 수 있다. 일반적으로, 분석 연산자는 숫자 또는 범주형과 같은 특정 데이터 타입에만 적용될 수 있다.

3.1 SameValue Analysis Operator

이 연산자는 어떠한 속성 그룹 AG_{A_i}내의 속성 값들이 모두 동일한지 여부를 판단한다. 일반적으로 민감 속성(SA)에 적용되어 민감 속성값들이 속성 연계 공격(예: 동질성 공격)에 취약한지 여부를 판단하는데 사용된다. 예를 들어, Table 5에는 세 개의 동질 클래스가 있으며 질병 속성 값들도 세 개의 속성 그룹인 $AG^{1_{disease}}, AG^2_{disease}$, $AG^3_{disease}$으로 분류된다. 첫 번째 속성 그룹 $AG^{1_{disease}}$은 "sameValue"라는 특성을 가지며 특성 속성 그룹 $FAG^{sameValue}_{disease}$로 표기된다.

3.2 SimilarValue Analysis Operator

이 연산자는 어떠한 속성 그룹내의 속성 값들이 의미적으로 서로 관련이 있는지를 판별한다. 본 연구에서는 의미적으로 유사한 단어를 포함하는 동의어 테이블(synonym table)을 구축한다. 예를 들어, 동의어 테이블에는 "폐암", "유방암", "혈액암"과 같이 "암" 카테고리에 속하는 의미적으로 유사한 단어들이 포함된다. 동의어 테이블은 사용자에 의해 수동으로 작성되거나 기존 문자열 변환 기법[20,21]을 통해 자동으로 구축될 수 있다. 예를 들어, [21]에서는 스프레드시트 내에서 문자열 처리를 입력-출력 예제를 사용하여 자동화하는 방법을 다루고 있다. 스프레드시트에서의 문자열 처리 작업(예: lung cancer-> cancer, breast cancer-> cancer 등)은 종종 번거롭고 복잡하며, 일반 사용자들에게는 프로그래밍적인 해결책을 구현하는 것이 어려울 수 있는데 이를 해결하기 위해, [21]

은 프로그래밍 언어를 사용하지 않고도 최종 사용자가 입력-출력 예제를 제공하여 문자열 처리 작업을 자동화할 수 있는 기술을 제안한다.

3.3 DifferentSensitivity Analysis Operator

이 분석은 속성 그룹 내의 민감 속성 값들이 다양한 민감도 수준을 나타내는지를 판별한다. 데이터 배포자는 속성 값을 평가하고 민감도 수준에 따라 속성 값의 순위를 매긴다. 개인의 프라이버시에 더 큰 위험을 노출하거나 더 큰 피해 가능성을 가지는 값들에 더 높은 민감도 수준을 할당한다. 이 연산자는 배포되는 데이터에서 민감한 값을 유추할 확률을 제한하려는 경우에 더욱 적합한 프라이버시 모델을 선택하는 데 도움이 될 수 있다[22]. 예를 들어, 민감 속성값 Diabetes, Flu, Asthma, HIV가 주어진 경우, 데이터 배포자가 HIV에 대해서 높은 민감도 수준을 할당하고 나머지 값들에 대해서는 낮은 민감도 수준을 할당한다고 가정하자. Table 5에서 분석 결과 첫 번째와 두 번째 속성 그룹은 동일한 수준의 민감 속성값들을 가지지만 세 번째 속성 그룹 $AG^3_{disease}$ 은 민감 속성값들이 서로 다른 수준의 민감도를 가지기 때문에 "differentSensitivity"라는 특성을 가지며 그 속성 그룹은 $FAG^{differentSensitivity}_{disease}$로 표기된다.

3.4 DuplicateRecord Analysis Operator

이 분석은 주어진 데이터에서 중복된 레코드의 존재 여부를 식별한다. 특정 속성을 기준으로 데이터를 오름차순이나 내림차순으로 정렬한다. 정렬을 통해 유사한 레코드들이 서로 인접하게 나열되어 레코드 중복 여부를 식별할 수 있다. 이 연산자는 특정 동질 클래스 내에서 여러 레코드들이 동일한 개인에 해당하는 상황에서 개인정보 유출의 가능성을 줄일 수 있는 프라이버시 모델을 선택하는 데 유용한 특성을 식별하는데 사용된다[23].

3.5 Skewness Analysis Operator

이 연산자는 속성 그룹 내에서 민감 속성값 분포의 쏠림(Skewness) 여부를 분석한다. 특정 민감 속성 값이 동질 클래스 내에서 다른 값보다 더 자주 나타나게 되면, 공격자로 하여금 그 동질 클래스에서 공격 대상이 해당 값을 가질 가능성이 매우 높다고 추론하도록 할 수 있다. 예를 들어, “Flu”에 걸리는 빈도가 “HIV”에 걸리는 빈도보다 훨씬 더 높은 경우를 예로 들수 있다.

특정 상황에서는 동질 클래스내의 민감 속성 값의 분포와 전체 데이터의 민감 속성 값 분포를 비교해야 할 필요가 있다. 예를 들어, 1000개의 레코드로 구성된 테이블에서 그 중 90%가 민감 속성 값으로 "Flu"를 가지고 있고 10%가 "HIV"를 가지고 있다고 하자. 이때 특정 동질 클래스내에 "Flu"인 속성 값이 90개, "HIV"인 속성 값이 10개가 있다고 가정하면, 특정 동질 클래스내의 분포가 쏠렸다고 할 수 있지만, 전체 데이터의 민감 속성 값 분포를 고려할 때 동질 클래스내의 민감 속성 값들이 쏠려있다고 결론 내리기는 어렵다. 이러한 두 분포 간의 거리를 계산하기 위해, 이전 연구에서와 마찬가지로 EMD(Earth Mover's Distance)를 활용한다[11,24]. EMD의 수식은 다음과 같다.

$$EMD = E[P,Q] = \frac{1}{2}\sum_{i=1}^{m} | p_i - q_i |$$

여기서 EMD 함수 E는 전체 민감 속성 확률 분포(P)와 특정 동질 클래스의 민감 속성 확률 분포(Q)를 받는다. 민감 속성값의 종류가 m개 있다고 했을 때, EMD는 전체 민감 속성값의 확률 $P = \{p_1,\ldots,p_m\}$와 특정 동질 클래스의 민감 속성값들의 확률 $Q = \{q_1,\ldots,q_m\}$의 차이를 모두 더한값에 2를 나누어 계산된다.

4. Privacy Model Recommendation using Privacy Model Background Knowledge

본 절에서는 프라이버시 모델 배경지식을 활용한 프라이버시 모델 추천 방안을 논의한다.

4.1 Privacy Model Background Knowledge

프라이버시 모델 배경지식(이하 PMBK)은 프라이버시 모델과 이러한 모델 선택 시 고려해야 할 데이터 특성에 대한 도메인 전문가(예: 데이터 배포자)의 지식과 경험을 표현한다. 도메인 전문가들은 프라이버시 모델의 사용 목적, 모델이 효과적으로 방어할 수 있는 공격, 모델에 적합한 데이터 유형 등에 대한 지식을 가지고 있을 수 있다. 예를 들어, k-익명성은 레코드 연계 공격에 효과적으로 대응할 수 있지만, 민감 속성 값들이 다양하지 않다면 속성 값을 보호하는 데 유용하지 않을 수 있다[9]. 반면에, l-다양성은 질병 속성 같은 범주형(Categorical) 민감 속성을 보호하는 데 유용하며, (α,k)-익명성은 민감 속성 값 추론에 대해 한계를 설정하는 데 적용될 수 있다[25].

Table 6는 본 연구를 위해 구축된 샘플 PMBK를 보여준다. PMBK는 (S_i, M_i) 튜플로 구성되며, 여기서 S_i는 프라이버시 모델 선택 시 고려해야 할 데이터 특성을 나타내고, M_i는 해당 특성 S_i를 갖는 데이터에 적합한 프라이버시 모델을 나타낸다. 예를 들어, Table 6에서 튜플 1은 특성 "sameValue"을 가진 데이터에 대해 l-다양성 모델이 제안된다는 것을 나타낸다.

Table 6. Sample Privacy Model Background Knowledge(PMBK)

Tuple	Feature Set(S_i^*)	Privacy Model(m_i^{**})	Ref
1	S_1= {sameValue}	m_1= *l*-diversity	[10]
2	S_2= {skewness}	m_2= *t*-closeness	[11]
3	S_3= {categorical, differentSensitivity}	m_3= (α,k)-anonymity...	[25]
4	S_4= {duplicateRecord}	m_4= *(X,Y)*-anoymity	[23]
5	S_5= {numerical, narrowRange}	m_5= (k,e)-anonymity...	[26]
6	S_6= {narrowRange, skewness}	m_6= *(e,m)*-anonymity	[27]
7	S_7= {sameValue, similarValue}	m_7= *t*-closeness	[11]

*Each feature set S_i belongs to *P*(F), which is a power set of F.
**Privacy model m_i belongs to M, which is a set of available privacy models.

Building the PMBK: 기본(Default) PMBK는 시스템의 초기 설정 시 구성되며, 특정 데이터셋에 종속적이지 않고 범용적으로 적용될 수 있다. PMBK는 도메인 전문가들의 경험이나 지식에 의해 구축되거나 혹은 기존 연구 문헌(예: [7,10,11,23,25,26,27])에 기반하여 구축될 수도 있다. 예를 들어, l-다양성(l-diversity)[10] 모델은 익명화 테이블 각각의 동질 클래스가 최소 l개의 민감 속성값을 가지도록 한다. 이 모델은 동질성 공격을 방어하는데 효과적인 모델이다. 만일 주어진 데이터셋의 특정 속성 그룹이 "sameValue" 특성을 가진다면 l-다양성 모델은 프라이버시를 보호하는데 효과적이다. 위의 l-다양성 모델은 쏠림 공격(Skewness Attack)과 유사성 공격(Similarity Attack)에 취약하다. 여기서, 쏠림 공격이란 전체 민감 속성값의 분포와 특정 동질 클래스 내의 민감 속성값 분포의 차이가 클 경우, 그 차이를 이용하여 공격하고자 하는 대상의 민감 속성값을 유추하는 공격이다. t-근접성(t-closeness) 모델[11]은 이러한 쏠림 공격과 유사성 공격 등에 대해 대처가 가능하다. t-근접성을 데이터에 적용하면 모든 동질 클래스들의 민감 속성값 분포가 전체 민감 속성값 분포와 비슷하게 변형이 되기 때문에, 쏠림 공격에 대처할 수 있다. 따라서, 데이터셋이 "skewness" 특성을 가지게 되면 적절한 프라이버시 모델로서 t-근접성이 추천될 수 있다. (α,k)-익명성 모델[25]는 민감 속성값들의 일부의 비율을 조절하면서 동시에 k-익명성을 만족시키는 모델이다. 이 모델은 k-익명성과 민감 속성값에 대한 신뢰도를 다루기 때문에 레코드 연계와 속성 연계 공격을 어느 정도 방어하는데 효과적이다. 이 모델에서는 민감 속성값들의 민감도를 다르게 설정해야 할 필요가 있는데, 이를 위해서 민감 속성값들을 "Sensitive"와 "Non-sensitive"로 분류하는 과정이 필요하다. 본 연구에서 구축된 PMBK에서는 만일 주어진 데이터셋의 특정 속성 그룹의 값들이 범주형이며 "differentSensitivity" 특성을 가진다면 (α,k)-익명성 모델이 추천된다. 이러한 기본 PMBK는 도메인 전문가들(예: 데이터 배포자)이 시스템을 사용하면서 경험이 축적되는 과정에서 배경 지식이 추가하거나 수정될 수 있다.

4.2 Privacy Model Recommendation

원본 데이터가 주어진 경우, 그에 적절한 모델을 선택하기 위해 앞절에서 설명한 PMBK를 활용한다. 본 연구에서는 주어진 데이터 *D*로부터 분석된 특성 F'과 PMBK를 입력으로 받아 출력으로 *D*에 적합한 프라이버시 모델을 추천하는 알고리즘(RecommendModel)을 제공한다. "RecommendModel" 알고리즘은 데이터 *D*로부터 분석된 특성 F'와 PMBK가 주어진 경우 PMBK의 각 튜플 t에 대해서 특성 집합 S를 구한다(라인 3). 그리고 두 집합 S와 F' 간의 일치 여부를 계산하는 matchCost 값을 계산한다(라인 4). 만약, S와 F'이 일치한다면 matchCost 값은 1이고, 그렇지 않으면 0이다. 만일 matchCost의 값이 1이면 튜플 t에서 정의된 프라이버시 모델을 구하고 이를 후보 모델(CM: Candidate Model) 집합에 입력한다(라인 5에서 7). PMBK의 모든 튜플이 고려될 때까지 위의 단계를 반복한다(라인 2에서 9). 마지막으로, 데이터셋 *D*에 적절한 후보 모델 집합 CM을 리턴한다(라인 10).

Table 7. Algorithm for recommending models

Algorithm: RecommendModel

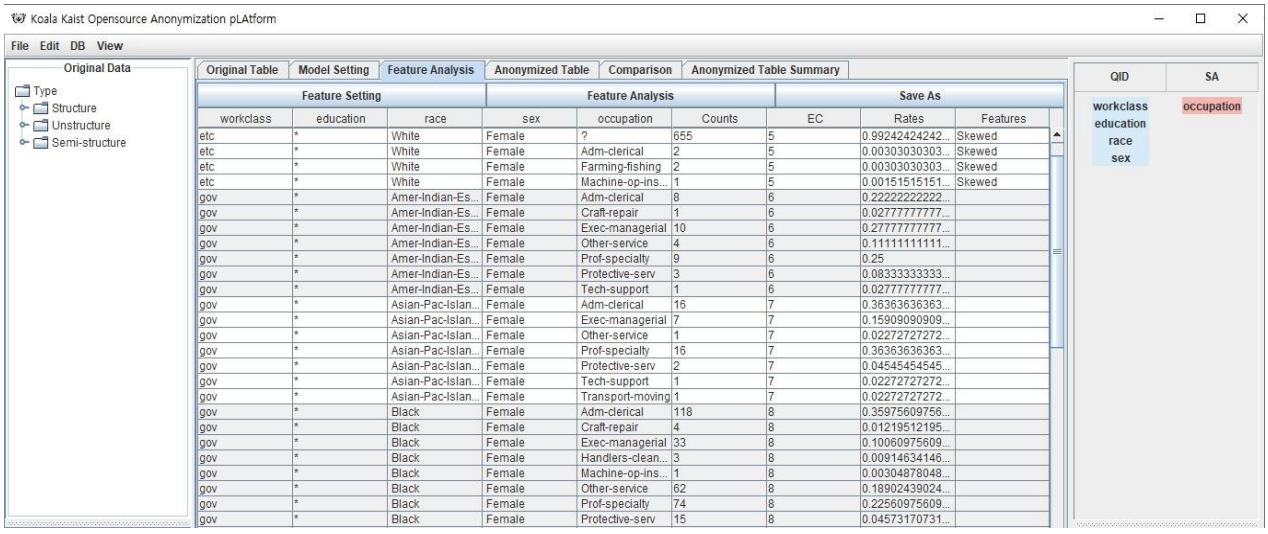
Input- Data features: F', Privacy model background knowledge: PMBK
Output- Candidate models: CM

```
1:  Let CM := ∅;
2:  foreach t ∈ PMBK do
3:      S := FeatureSet(t);
4:      compute matchCost(S, F');
5:      if matchCost(S, F')= 1 then
6:          m := PrivacyModel(t);
7:          CM:= CM ∪ m;
8:      endif
9:  endFor
10: return CM;
```

5. Implementation, Usage, and Evaluation

5.1 Implementation

개발된 시스템은 Java와 J2EE 및 PostgreSQL 12 데이터베이스 엔진을 사용하여 구현되었으며, III.1절(Overall Process)에서 기술하였듯이 데이터 특성 분석, 모델 추천,



workclass	education	race	sex	occupation	Counts	EC	Rates	Features
etc	*	White	Female	?	655	5	0.99242424242...	Skewed
etc	*	White	Female	Adm-clerical	2	5	0.00303030303...	Skewed
etc	*	White	Female	Farming-fishing	2	5	0.00303030303...	Skewed
etc	*	White	Female	Machine-op-ins...	1	5	0.00151515151...	Skewed
gov	*	Amer-Indian-Es...	Female	Adm-clerical	8	6	0.22222222222...	
gov	*	Amer-Indian-Es...	Female	Craft-repair	1	6	0.02777777777...	
gov	*	Amer-Indian-Es...	Female	Exec-managerial	10	6	0.27777777777...	
gov	*	Amer-Indian-Es...	Female	Other-service	4	6	0.11111111111...	
gov	*	Amer-Indian-Es...	Female	Prof-specialty	9	6	0.25	
gov	*	Amer-Indian-Es...	Female	Protective-serv	3	6	0.08333333333...	
gov	*	Amer-Indian-Es...	Female	Tech-support	1	6	0.02777777777...	
gov	*	Asian-Pac-Islan...	Female	Adm-clerical	16	7	0.36363636363...	
gov	*	Asian-Pac-Islan...	Female	Exec-managerial	7	7	0.15909090909...	
gov	*	Asian-Pac-Islan...	Female	Other-service	1	7	0.02272727272...	
gov	*	Asian-Pac-Islan...	Female	Prof-specialty	16	7	0.36363636363...	
gov	*	Asian-Pac-Islan...	Female	Protective-serv	2	7	0.04545454545...	
gov	*	Asian-Pac-Islan...	Female	Tech-support	1	7	0.02272727272...	
gov	*	Asian-Pac-Islan...	Female	Transport-moving	1	7	0.02272727272...	
gov	*	Black	Female	Adm-clerical	118	8	0.35975609756...	
gov	*	Black	Female	Craft-repair	4	8	0.01219512195...	
gov	*	Black	Female	Exec-managerial	33	8	0.10060975609...	
gov	*	Black	Female	Handlers-clean...	3	8	0.00914634146...	
gov	*	Black	Female	Machine-op-ins...	1	8	0.00304878048...	
gov	*	Black	Female	Other-service	62	8	0.18902439024...	
gov	*	Black	Female	Prof-specialty	74	8	0.22560975609...	
gov	*	Black	Female	Protective-serv	15	8	0.04573170731...	

Fig. 2. Result of performing data feature analysis on “Adult” dataset

데이터 비식별화 세 개의 모듈로 구성되어 있다. Table 8은 이러한 모듈이 동작하면서 호출하는 몇몇 주요 함수들을 나타내준다. 시스템은 비식별화 도구로 잘 알려져 있으며 오픈 소스인 ARX[3]를 기반으로 개발되었으며, 프라이버시 모델 (예: *k*-익명성, *l*-다양성, *t*-근접성, 차분프라이버시 등)을 구현하기 위해 ARX가 제공하는 API를 사용하였다. 또한, 시스템은 원본 데이터 탐색, 데이터 분석 수행, 프라이버시 모델 및 관련 파라미터 설정, 비식별된 결과 탐색 등을 위한 GUI를 제공한다.

Table 8. Operation list

Data feature analysis
- *extractFeature*(A_i, op)} identifies a feature with a feature analysis operator op from attribute A_i. - *checkFeature*(AG_i, f)} checks whether attribute group AG_i has a feature f. - *generateAttributeGroups*(D)} returns a set of attribute groups from given D.
Model recommendation or Data de-identification
- *recommendModels*(D)} returns a set of privacy models appropriate to D. - *chooseParameter*(p, m)} allows users to choose a parameter p for model m. - *de-identifyData*(D, m) de-identifies dataset D with a recommeded model m.

5.2 Usage Scenario

Fig.2는 Adult 데이터셋[28](III.5.3에서 설명)에 특성 분석을 수행한 결과 화면을 보여준다. 전체 화면은 크게 세 개의 패널로 구성되어 있다. 왼쪽 패널은 데이터 유형별로 분류된 데이터셋을 트리 구조로 보여준다. 만약 사용자가 트리의 한 노드를 선택하게 되면 시스템은 노드에 해당하는 원본 데이터셋을 DB로부터 로딩하여 화면 중앙에 보여준다. 사용자는 “Original Table” 탭에서 원본 데이터의 속성 이름, 속성 타입, 속성 값, 레코드의 개수 등 세부 정보를 파악할 수 있다. “Model Setting” 탭에서 사용자는 원본 데이터의 속성들 중에서 준식별자 및 민감 속성 선택을 선택한다. Fig.2의 우측 패널은 사용자가 Adult 데이터셋에서 준식별자로 “workclass”, “education”, “race”, “sex”, 민감 속성으로 “occupation”을 선택하였음을 보여준다. 또한 “Model Setting” 탭은 사용자로 하여금 프라이버시 모델과 그와 관련된 파라미터 설정, 선택된 준식별자의 일반화를 위한 계층 트리(Hierarchy Tree) 등을 설정할 수 있도록 한다.

원본 데이터에서 준식별자와 민감 속성이 지정된 후 사용자는 화면 중앙의 "Feature Analysis" 탭에서 데이터 특성 분석을 수행한다. 사용자가 데이터 특성 관련 셋팅 (예: threshold)을 하고 “Feature Analysis” 버튼을 누르게 되면 시스템은 주어진 데이터에 대해서 특성 분석을 수행한다. Fig.2의 분석 결과 화면은 민감 속성으로 선택된 "occupation"은 "skewness" 특성을 가진다는 것을 보여준다. Table 6의 PMBK에 따르면 주어진 데이터셋이 “skewness” 특성을 가지면 적절한 프라이버시 모델로서 *t*-closeness가 추천된다.

따라서, 사용자는 추천된 *t*-closeness 모델을 사용하여 Adult 데이터셋을 비식별화하며 비식별화된 결과는 Fig.3에 주어져 있다. Fig.3에서 보여지는 바와 같이 비식별화된 데이터는 여러 개의 동질 클래스로 구성되며 동질 클래스의 준식별자 값은 서로 동일함을 알 수 있다. *t*-closeness 모델에서 파라미터 “t” 값 선택은 개인정보 보호와 데이터 유용성 사이의 균형을 달성하기 위한 중요한 결정이며 “t” 값은 0에서 1사이의 값을 가지며 주어진 동질 클래스 내의

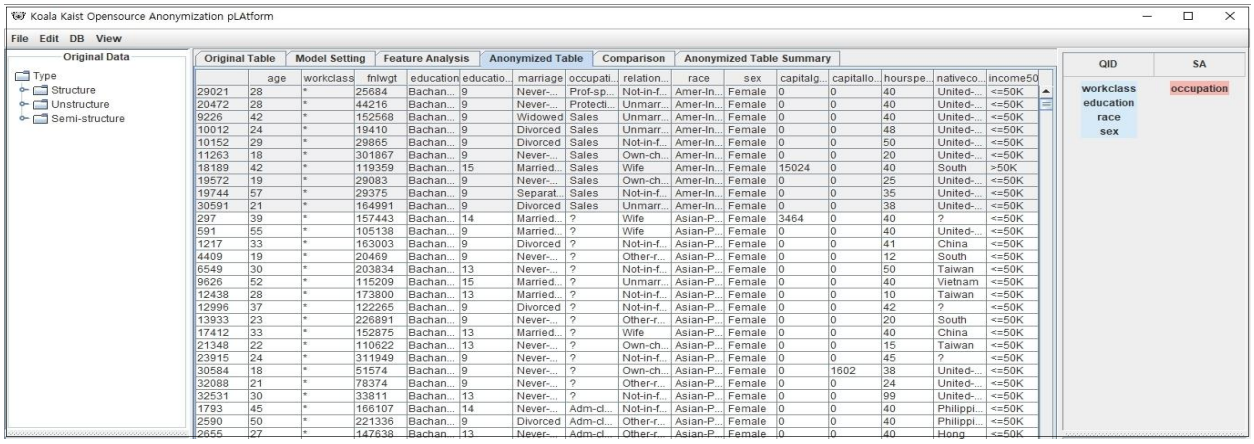


Fig. 3. Result of de-identifying the original "Adult"dataset using t-closeness(t= 0.2)

민감한 속성 분포와 전체 데이터셋 내의 분포 사이의 유사성 수준을 결정한다. 낮은 "t" 값은 보다 엄격한 개인정보 보호를 제공하지만 데이터 유용성 손실을 가져올 수 있다. 적절한 "t" 값을 선택하기 위해 "t" 값을 점진적으로 조정하면서 개인정보 보호와 데이터 유용성에 미치는 영향을 평가한다. 본 연구에서는 "t"의 값을 0.1~ 0.9까지 0.1 단위로 변경하며 실험을 수행하였으며 Fig.3은 비식별화된 결과의 예제로서 여러 실험 중 "t"의 값을 0.2로 설정했을 때의 결과를 보여준다. 또한, 최적의 "t" 값을 선택하는 문제는 NP-hard 문제로 알려져 있다[29].

5.3 Evaluation

Dataset: 개발된 시스템의 성능 평가를 위해 본 논문에서는 UC Irvine 기계학습 저장소(machine learning repository)에서 제공하는 Adult 데이터셋[28]을 사용하였다. Adult 데이터셋은 미국 성인 인구의 다양한 속성(예: 나이, 교육 수준, 직업, 성별, 인종 등)과 소득 수준 정보(50K 이상 또는 50K 미만)를 포함하고 있으며 총 32,560개의 행으로 구성되어 있다. 이 데이터셋은 이전 프라이버시 보호 관련 연구[11,25,26,30,31,32]에서 시험 평가를 위해 자주 활용되어 왔다. 표 9는 Adult 데이터셋의 주요 속성을 보여준다.

Table 9. Description of main attributes in Adult dataset

	Attribute	Type	Distinct Values
1	Work class	Categorical	8
2	Education	Categorical	16
3	Race	Categorical	5
4	Sex	Categorical	2
5	Age	Numeric	74
6	Country	Categorical	41
7	Marital status	Categorical	7
8	Salary	Sensitive	2
9	Occupation	Sensitive	14

Evaluation Metrics and Methodology:

본 논문에서는 비식별화된 데이터의 유용성을 판단하기 위한 지표로 분별력 척도(DM: Discernibility Metric)[7,10,33]를 사용한다. DM은 비식별화된 데이터의 모든 동질 클래스의 크기를 제곱하여 더한 값으로 값이 클수록 데이터 유용성이 떨어진다. DM의 수식은 다음과 같이 표현된다.

$$DM(T) = \sum_{i=1}^{n} | EC_i |^2$$

여기서 T는 비식별화된 데이터를 의미하며 EC_i는 동질 클래스를 나타낸다. T의 DM은 모든 동질 클래스의 크기의 제곱의 합으로 계산된다.

본 실험에서는 쏠림(skewness) 취약점을 갖고 있는 Adult 데이터셋에 개발된 추천 시스템이 특성 분석을 통해 추천한 모델인 t-근접성을 적용한 비식별 결과와 프라이버시 보호를 위해 널리 사용되고 있는 k-익명성과 l-다양성을 적용한 결과를 프라이버시 보호 측면과 데이터 유용성 측면에서 비교 분석하였다. 데이터 유용성 비교를 위해 위에서 설명한 DM을 사용하였으며 프라이버시 보호 비교를 위해 Adult 데이터셋이 가지고 있는 쏠림 취약점이 비식별화된 결과에서 효과적으로 제거되었는지를 확인한다. 본 실험에서는 Adult 데이터셋에서 준식별자로 "work class", "education", "race", "sex", 민감 속성으로 "occupation"을 사용하였다. 프라이버시 모델 적용을 위해 ARX API를 활용하였으며, 일반화를 위해 전역 일반화 (Global Generalization)을 적용하였다.

Result: Fig. 4는 Adult 데이터셋에 k-익명성, l-다양성, t-근접성 모델을 적용하여 비식별화한 결과의 DM값을 보여준다. 위 그림에서 알 수 있듯이 k-익명성과 l-다양성의 경우에는 k와 l의 값이 증가할수록 DM값이 계단식으로 증가(데이터 유용성 감소)한다. 반면에 t-근접성의 경우에

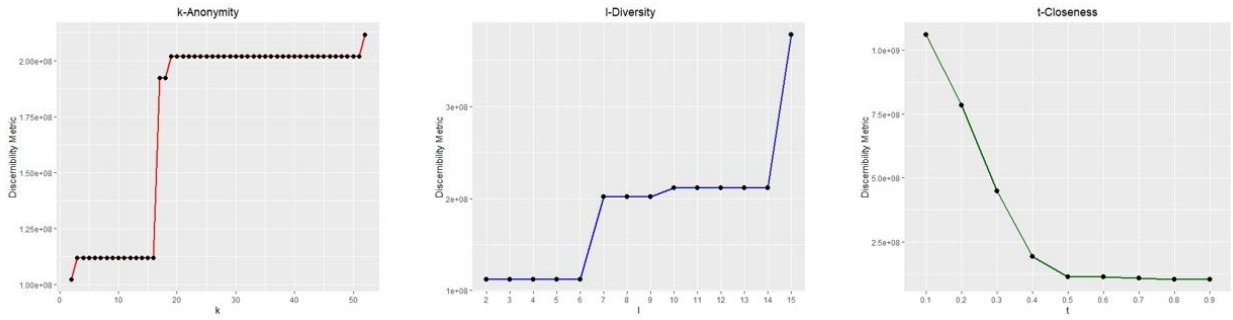


Fig. 4. Data utility of k-anonymity, l-diversity, and t-closeness using varying parameters in Adult dataset

는 t의 값이 감소할수록 DM값이 증가하는 것을 알 수 있다. Fig. 4에서 동일한 DM값을 나타내는 점(point)들은 비식별화된 결과가 같다는 것을 의미한다. 예를 들어, k-익명성(k = 3~17) 경우 k값이 3부터 17까지 변화할 때 동일한 DM값을 가지며 각각의 경우 비식별화된 결과는 같다.

Table 10. DM vs. number of skewed EC

Model	DM	Number of skewed EC
k-anonymity (k= 3~17)	1.1e+08	5 out of 16 (31%)
k-anonymity (k= 19~51)	2.0e+08	3 out of 16 (19%)
l-diversity (l= 2~6)	1.1e+08	5 out of 16 (31%)
l-diversity (l= 7~9)	2.0e+08	3 out of 16 (19%)
l-diversity (l= 10~14)	2.1e+08	1 out of 6 (17%)
t-closeness (t= 0.4)	1.9e+08	0 out of 18 (0%)

Table 10은 Fig. 4의 각 모델을 적용한 결과의 DM값과 쏠림 취약점에 대한 노출 정도를 요약한 표이다. Table 10에서 "Number of skewed EC" 열은 비식별화된 결과에서 쏠림 취약점에 노출된 동질 클래스의 수를 나타낸다. 예를 들어, k-익명성의 경우 k의 값이 3에서 17까지 변화할 때 동일한 DM값(1.1e+08)을 가지며 각각의 비식별화된 결과는 16개의 동질 클래스로 구성되며 그 중 5개가 쏠림 취약점에 노출된다는 것을 의미한다. Table 10에서 k-익명성과 l-다양성 모델의 경우 매개변수의 값을 늘리면서 프라이버시 보호 정도를 증가시켜도 쏠림 취약점이 완전히 사라지지 않는 것을 볼 수 있다. 오히려 DM값이 늘어나면서 데이터의 유용성을 감소시킨다.

하지만, t-근접성은 t = 0.4일 때 k = 19~51일 때의 k-익명성의 DM값(2.0e+08), 그리고 l = 10~14 일 때의 l-다양성의 DM값(2.1e+08)과 비교했을 때 다소 낮은 DM값(1.9e+08)을 가지지만 쏠림 취약점이 존재하지 않는다. 즉, 본 연구에서 개발된 추천 시스템이 데이터 특성 분석에 기반하여 추천한 t-근접성이 k-익명성과 l-다양성에 비해 데이터의 유용성을 유지하면서 쏠림 취약점을 제거하는데 더 효과적이라는 것을 보여준다. 이는 기존 연구에서 쏠림 취약점에 대응 할때 k-익명성과 l-다양성보다 t-근접성이 더 효율적이라는 주장을 뒷받침하는 결과라 볼 수 있다.

IV. Conclusion and Future Work

사용자가 선택할 수 있는 프라이버시 모델의 수가 많고 또한 데이터의 특성이 다양한 환경에서 최적의 프라이버시 모델을 선택하는 것은 상당한 노력과 전문지식이 필요하다. 본 논문에서는 주어진 데이터에 대해 개인의 개인정보를 보호하는 데 최적의 프라이버시 모델을 추천하는 시스템을 개발하였다. 이 시스템은 사용자로 하여금 주어진 데이터의 특성을 분석하도록 지원하며 분석된 특성에 기반하여 적합한 프라이버시 모델을 추천하여 데이터를 비식별화한다. 특히, 데이터의 사이즈가 크고 데이터의 특성이 다양한 경우에 고도화된 전문지식을 갖춘 데이터 배포자라 할지라도 주어진 데이터에 적합한 프라이버시 모델을 선정하는 것은 어려운 문제이다. 이러한 경우에 본 연구에서 개발된 추천 시스템은 데이터 배포자가 보다 쉽게 프라이버시 모델을 선택하여 주어진 데이터를 비식별화하는데 유용하게 사용될 수 있다. 향후 연구에서는 좀 더 다양한 데이터 특성 분석과 모델들을 다룰 예정이며 텍스트, 이미지, 비디오, 오디오와 같은 다른 유형의 데이터에 대해 개발된 시스템을 적용할 수 있도록 확장하고 더욱 고도화할 계획이다.

ACKNOWLEDGEMENT

This work was developed with the support of Global Cybersecurity Research grant (Project ID: 1711177169) from the Ministry of Science and ICT, Republic of Korea.

REFERENCES

[1] M. H. Afifi, K. Zhou, and J. Ren, "Privacy characterization and quantification in data publishing," IEEE Trans. Knowl. Data Eng., 30(9):1756-1769, 2018. DOI: 10.1109/TKDE. 2018.2797092

[2] L. Yao, Z. Chen, X. Wang, D. Liu, and G. Wu, "Sensitive label privacy preservation with anatomization for data publishing," IEEE Trans.Dependable Secur. Comput., 18(2):904-917, 2021. DOI: 10.1109/TDSC.2019.2919833

[3] F. Prasser, J. Eicher, H. Spengler, R. Bild, and K. A. Kuhn, "Flexible data anonymization using ARX - current status and challenges ahead," Softw. Pract. Exp., 50(7):1277-1304, 2020. DOI: 10.1002/spe.2812

[4] G. Kim, "Two Fundamental Questions in AI Ethics: With a Reflection on AI Chatbot Iruda," Transdisciplinary Humanities, vol., no.10, pp 39-76, 2022 (in Korean). DOI: 10.37123/th.2022. 10.39

[5] Seunghwan Kim, Sunghae Jun, "Dig Data Integration using Data De-identification," Journal of Korean Institute of Intelligent Systems, 29(3), pp. 235-241, 2019. DOI: 10.5391/JKIIS.2019.29. 3.235

[6] S.H. Eom, I.K. Lee, W.G Lee, "BigData-based Trend of Personal Information De-identification," Korea Institute of Enterprise Architecture, 15(4), 545-552, 2018 (in Korean). DOI: 10.22865/ jita.2018.15.4.545

[7] B. C. M. Fung, K. Wang, R. Chen, and P. S. Yu, "Privacy-preserving data publishing: A survey of recent developments," ACM Comput. Surv., 42(4):14:1-14:53, 2010. DOI: 10.1145/1749603.1749605

[8] A. Majeed, S.C. Lee, "Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey," IEEE Access 9: 8512-8545, 2021. DOI: 10.1109/ACCESS. 2020.3045 700

[9] L. Sweeney, "k-anonymity: A model for protecting privacy," Int. J. Uncertain. Fuzziness Knowl. Based Syst., 10(5):557-570, 2002. DOI: 10.1142/S0218488502001648

[10] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasub ramaniam, "l-diversity: Privacy beyond k-anonymity," In Proceedings of the 22nd International Conference on Data Engineering, 2006. DOI: 10.1109/ICDE. 2006.1

[11] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," Proceedings of the 23rd International Conference on Data Engineering, 2007. DOI: 10.1109/ICDE.2007.367856

[12] Cynthia Dwork, "Differential Privacy," 33rd International Colloquium on Automata, Languages and Programming, Part II (ICALP), 2006. DOI: 10.1007/11787006_1

[13] W. Mahanan, W. A. Chaovalitwongse, and J. Natwichai, "Data privacy preservation algorithm with k-anonymity," World Wide Web, 24(5):1551-1561, 2021. DOI: 10.1007/ s11280-021-00922-2

[14] D. Slijepcevic, M. Henzl, L. D. Klausner, T. Dam, P. Kieseberg, and M. Zeppelzauer, "k-anonymity in practice: How generalisation and suppression affect machine learning classifiers," Comput. Secur., 111:102488, 2021. DOI: 10.1016/j.cose.2021.102488

[15] Jongseon Kim, Kijung Jung, Hyukki Lee, Soohyung Kim, Jong Wook Kim, and Yon Dohn Chung, "Models for Privacy-preserving Data Publishing : A Survey," Journal of KIISE, 44(2), 2017 (in Korean). DOI: 10.5626/ JOK.2017.44.2.195

[16] A. Majeed and S. O. Hwang, "Rectification of Syntactic and Semantic Privacy Mechanisms," in IEEE Security & Privacy, 2022. DOI: 10.1109/MSEC.2022.3188365

[17] M. Cunha, R. Mendes, J. P. Vilela. "A survey of privacy-preserving mechanisms for heterogeneous data types," Computer Science Review, 2021.

[18] Ministry of Science and ICT(MSIT) and National Information Society Agency(NIA), "Privacy Deidentification Technique Guideline," 2019. (In Korean)

[19] K Psaraftis, T Anagnostopoulos, K Ntalianis, N Mastorakis, "Customized Recommendation System for Optimum Privacy Model Adoption", International Journal of Economics and Management SystemsA, 2018. DOI: 10.52950/iaras.2018.1.001

[20] A. Arasu, S. Chaudhuri, and R. Kaushik, "Learning string transformations from examples," Proceedings of the Very Large Database (VLDB) Endowment, 2(1):514-525, 2009. DOI: 10.14778/2212351.2212356

[21] Sumit Gulwani, "Automating string processing in spreadsheets using input-output examples", Symposium on Principles of Programming Languages, 2011. DOI: 10.1145/1926385.1926423

[22] K. Wang, B. C. M. Fung, and P. S. Yu, "Handicapping attacker's confidence: an alternative to k -anonymization," Knowl. Inf. Syst., 11(3):345-368, 2007. DOI: 10.1007/ s10115-006-0035-5

[23] Ke Wang, Benjamin Fung, "Anonymizing sequential releases," ACM SIGKDD, 2006. DOI: 10.1145/1150402.1150449

[24] Y. Rubner, C. Tomasi, and L. J. Guibas, "The earth mover's distance as a metric for image retrieval", Int. J. Comput. Vis., 40(2):99-121, 2000. DOI: 10.1023/ A:1026543900054z

[25] R. C. Wong, J. Li, A. W. Fu, and K. Wang, "(alpha, k)-anonymity: an enhanced k-anonymity model for privacy preserving data publishing," SIGKDD, 754-759, 2006. DOI: 10.1145/1150402. 1150499

[26] Qing Zhang, Nick Koudas, Divesh, Srivastava, Ting Yu, “Aggregate Query Answering on Anonymized Tables,” ICDE, 2007. DOI: 10.1109/ICDE.2007.367857

[27] Jiexing Li, Yufei Tao, Xiaokui Xiao, “Preservation of Proximity Privacy in Publishing Numerical Sensitive Data," SIGMOD, pp 473-486, 2008. DOI: 10.1145/1376616. 1376666

[28] UCI Machine Learning Repository, www.archive.ics.uci.edu

[29] Hongyu Liang, Hao Yuan, “On the Complexity of t-Closeness Anonymization and Related Problems", DASFAA, 2013. DOI: 10.1007/978-3-642-37487-6_26

[30] JM. H. Afifi, Kai Zhou, Jian Ren, “Privacy Characterization and Quantification in Data Publishing," IEEE Trans. Knowl. Data Eng., 30(9), 2018. DOI: 10.1109/TKDE.2018.2797092

[31] Chaobin Liu, Shixi Chen, Shuigeng Zhou, Jihong Guan, Yao Ma, “A general framework for privacy-preserving of data publication based on randomized response techniques", Inf. Syst., 96, 2021. DOI: 10.1016/j.is.2020.101648

[32] Djordje Slijepcevic, Maximilian Henzl, Lukas Daniel Klausner, Tobias Dam, Peter Kieseberg, Matthias Zeppelzauer, “k-Anonymity in practice: How generalisation and suppression affect machine learning classifiers", Computers & Security, 111, 2021. DOI: 10.1016/j.cose.2021.102488

[33] A. Skowron and C. Rauszer. “Intelligent Decision Support: Handbook of Applications and Advances of the Rough Set Theory,” Chapter The Discernibility Matrices and Functions in Information Systems, 1992. DOI:https://doi.org/10.1016/0377-2217(94)90431-6

Authors

Seung Hwan Ryu received the Master's and Ph.D. degrees in Computer Engineering from the University of New South Wales, Australia, in 2007 and 2013 respectively. He worked as a research associate in the School of Computer Engineering at the University of New South Wales from 2012 to 2013. He also served as an adjunct lecturer at the same university from 2015 to 2019. After that, he worked as the head of the Big Data Security Research Institute at Egloo Security from 2019 to 2022. Currently, he is a principal researcher at the KAIST Cyber Security Research Center. Research interests include data matching, privacy protection, AI security, and information systems security.

Yongki Hong received the B.S degree from the Department of Statistics, University of California Los Angeles in 2022. He is currently a researcher in KAIST Cyber Security Research Center. He is interested in data science, privacy, and AI.

Gihyuk Ko received M.S. and B.S. degrees in Electrical and Computer Engineering at Carnegie Mellon University and Seoul National University, respectively. He is a Ph.D. Candidate in Electrical and Computer Engineering at Carnegie Mellon University and a research scientist in Cyber Security Research Center at KAIST. His research interests include Privacy, Security, and Fairness in Machine Learning Models, Formal Methods, and Artificial Intelligence.

Heedong Yang received the B.S. and M.S. degrees from the Department of Computer Engineering, Hannam University, Korea, in 2021. He is currently a researcher in KAIST Cyber Security Research Center. His research interests include binary analysis, privacy, and system security.

Jong Wan Kim received the Ph.D. degree in Computer Science and Engineering from Korea University, South Korea, in 2007. He researched at the University of New South Wales (UNSW), Sydney, Australia from 2012 to 2013 as a visiting fellow. Dr. Kim joined the faculty of the Smith College of Liberal Arts in 2016 and works for Software Convergence Education Center at Sahmyook University from 2021, respectively. He is currently a professor and he is interested in Big Data, Machine Learning and Distributed Computing.