통계 배경 지식을 이용한 추론 공격에서 프라이버시를 지키는 익명화 기법

류영하 정강수O 박석
서강대학교 컴퓨터공학과
ywenry@naver.com, azure84@naver.com, spark@sogang.ac.kr

An Anonymization Technique with Preserving Privacy against Inference Attack using Statistical Background Knowledge

Younha Ryu Kangsoo JungO, Seog Park
Department of Computer Science and Engineering, Sogang University

1. 서 론

기업과 조직은 연구와 마케팅 등의 다양한 목적을 위하여 각종 정보를 수집하고 이를 공공의 목적으로 배포하여 왔다. 시간의 흐름에 따라 데이터 누적의 양이 커지면서 정보 노출에 의한 피해 사례도 증가하였고 두 개 이상의 서로 다른 목적으로 배포된 자료간의 공통속성을 비교해, 사용자의 개인 정보를 파악할 수 있는 추론 공격(Inference attack) 가능성이 새롭게 제시되었다[1]. 이를 방지하기 위하여 추론 공격에 대한 연구[2,3,4]가 점차적으로 진행되었으나 최근 공격 모델의 패러다임이 변화함에 따라 데이터를 보호하기 위한 익명화 기법의 변화가 요구되고 있다. 이제 공격자의 추론 공격은 복수개의 공개된 자료의 단순 비교에서 벗어나 각 데이터가 지닌 고유의 기반 지식을 이용해 프라이버시를 누출시키는 형태로 발전하고 있다[5]. 그러나 통계 배경 지식의 경우 공격 모델로써의 통계를 이용한 데이터 프라이버시의 누출 여지가 많음에도 불구하고, 이에 대한 연구가 전무한 실정이다. 본 논문은 통계에 의한 배경 지식을 근거로 한 새로운 공격 모델의 정의와 이에 대비해 개개인의 프라이버시를 보호하기 위한 새로운 익명화 알고리즘 기법에 초점을 맞춘다.

2. 본문

기빈 자식을 이용한 익명화 기법은 현재 데이터 통계 특성을 이용한 기반 지식에 맞추어져 있으며, 이 통계자료를 바탕으로 새로운 익명화 기법도 계속 연구되고 있다. 현재 기반 지식 분야에서 이슈가 되고 있는 통계를 이용한 기반지식 공격은 기존의 익명화 기법만으로는 데이터의 프라이버시 보호가 불가능하다. 예를 들어 하나의 튜플이 다른 튜플들에 비해 높은 확률값을 가진다면 공격자는 확률의 절대적 수치와는 관계없이 다른 튜플들과의 확률을 비교하여 특정 값을 추론할 수 있다. 만약 서로 다른 튜플들이 확률적으로 큰 차이가 있다면 확률적 추론 공격에 의해 쉽게 프라이버시 노출된다. 따라서 각 튜플의 확률 값을 고려해 비슷한 확률등르 가진 튜플들이 하나의 블록에 삽입되는 익명화 기법이 필요하다. 이 때, 확률적 추론을 통해 특정 값이 확실히 추론되었다면 남은 튜플을 이용해 추가적인 추론 공격이 가능하다. 이를 연속적인 확률적 추론 공격이라 정의한다.

[정의 1] 연속적인 확률적 추론 공격(Continuous Probability Inference Attack)

기존의 확률적 추론 공격에 의해 튜플의 프라이버시가 밝혀진 경우, 하나의 블록 안에 있는 튜플 간의 상대적 확률 관계가 달라짐에 따라, 연속적인 확률적 추론 공격이 가능하게 되어 블록 안의 모든 튜플의 프라이버시가 노출된다.

즉, 공격 모델을 기존의 Bucketlization 익명화 기법에 도입하면, 테이블에 있는 모든 튜플의 질병 프라이버시가 드러나게 되며 이외의 익명화 기법 또한 대부분 확률적 추론 공격을 취약성을 지니므로 데이터의 안정성을 보장할 수 없다. 따라서 특정 값에 대한 비슷한 확률을 지닌 튜플이 복수 개 존재하여 통계 배경 지식을 통한 추론 공격을 막기 위한 익명화 기법이 필요하다. 이러한 익명화 익명화 상태를 Sagety State라 정의한다.

[정의 2] Safety state

각 블록의 질병에 해당할 확률이 비슷한 튜플이 최소한 2개 이상인 경우, 해당 질병은 Safety state에 해당한다고 정의한다. 또한 블록 안에 있는 모든 질병이 Safety state에 해당할 경우, 해당 블록은 연속적인 확률 추론 공격으로부터 안전하다.

본 논문은 모든 익명화 그룹이 Safety state를 유지하도록 하기 위한 익명화 기법을 제시한다. 이를 위해 하나의 튜플이 복수개의 칼럼을 가지고 있는 환경을 고려하였으며, 하나의 블록이 지닐 수 있는 확률값 차이의 최대 허용치를 두어 연속적으로 추론될 수 있는 가능성을 차단한다.

각각의 익명화 그룹에 삽입되는 튜플들은 자신과 같은 블록 안에 속한 다른 튜플들의 확률이 서로의 확률적 임계값에 포함되는지를 확인해야 한다. 모든 SE 값에 대한 확률을 비교하는 것은 무의미하며, 각 블록에 해당하는 ST 테이블에 속한 SE 값에 대한 확률만을 고려한다. 확률적 임계 값을 감안하여 하나의 블록안에 튜플을 삽입할 때 다음 두 가지 점을 유의해야 한다.

(1)하나의 블록안에 존재하는 모든 SE 값이 Safety state를 형성해야 한다.
(2)이미 Safety state를 이룬 SE 값이 존재할 때, 추가로 삽입된 튜플이 Safety state를 훼손해서는 안된다.
제안 기법의 익명화 알고리즘은 다음과 같다.

```
Algorithm
Input : T(data in database to be anonymized, Having QI, SE value)
        K(parameter for K-anonymity, user configure)
        Max-threshold
        (parameter for probability threashold value, user configure)
        Min-threshold
        (parameter for probability threashold value, user configure)
Output : T'(anonymized bucket table of table T)
1: Check the all tuple which has highest probability of SE value.
2: Check the K-anonymity and Max,Min threshold
   2.1:form Block using tuple which has Highest probability of SE
       value.
   2.2:insert the other tuple(consider k,Max,Min and L-diversity)
   2.3:create the probability meta data.
   2.4:repeat form Block using other tuples.
3:Check the remain tuple.
   3.1:create block among remain tuples.
   3.2:check the probability meta data, and insert to block.
   3.3 check the remain tuple and search the adequate block.
4:Publish anonymized table T'
```

각 블록은 확률적 임계 값을 유지하기 위한 메타 데이터를 유지하며 튜플을 블록에 삽입할 때, 블록이 지닌 확률 메타데이터와 비교를 하여, 튜플이 삽입된 이후 Safety state가 유지될 수 있는 지를 확인한다. 본 제안 기법의 장점은 기존의 Bucketlization table 구조에 임계 값 메타 데이터만을 추가하였으며, 기존 기법의 알고리즘을 크게 수정하지 않고 적용할 수 있다는 점이다. 기존의 익명화 기법들이 l-diversity를 이용해 튜플의 블록 삽입에 제한을 두었다면, 제안 기법은 이에 확률적 임계 값에 의한 제약을 추가하였다.

이에 대한 실험을 위해 사용한 데이터는 UC Irvine machine learning repository[6]의 성인 데이터를 사용하였으며 Anatomy에서 제시한 Bucketlization 기법과의 비교를 위하여 동일한 Bucketlization 테이블의 구조를 사용하였다. 실험 환경은 Pentium IV 3.00GHZ 프로세서와 1GB DDR2 메모리 2개가 장착된 마이크로소프트 윈도우 XP 프로페셔널 2002버전 사양의 PC에서 실험하였다. 사용 언어는 Java이며 자바 가상 머신 1.6.0을 사용하였다. 또한 수집한 성인 데이터 중 질병에 대한 명확한 확률데이터를 가지고 있는 국가 속성을 지닌 30000개의 튜플을 실험 대상으로 사용하여 기존의 기법에 비해 나은 프라이버시 보호를 보장함을 보였다.

3. 결론

본 연구는 기반 지식 공격 모델을 대상으로 개인의 프라이버시를 보호하기 위한 익명화 기법에 대하여 설명하였다. 기존의 연구가 통계 자료를 배제한 QI 값의 공통속성만을 이용한 공격 모델만을 가정하였다는 전제하에 지식 기반 공격 모델을 감안한 익명화 기법에 대한 연구를 진행하였다. 본 논문에서 기여한 부분은 다음과 같다. 첫째, 기반 지식에 의한 공격 모델을 정의하였다. 지금까지 익명화 연구는 기반 지식에 의한 정확한 공격 모델을 제시하지 못하였던데 반해 본 논문에서는 각종 통계와 연속적인 상대 확률적 공격을 통한 공격 모델을 정확하게 제시하고 있다. 둘째, Safety state의 정의를 통한 익명화 기법을 제시하였다. 확률적 접근도가 비슷한 튜플들을 하나의 블록으로 묶어 각각의 튜플에 대한 추론 공격을 방지하여 프라이버시를 강화하는 효과를 얻을 수 있었다.

4. 참고문헌

[1]W.E Winkler, “Matching and Record Linkage”, Business survey methods, Wiley, Chichester, 1995.
[2]Latanya Sweeney, “Guaranteeing Anonymity when Sharing Medical Data the Datafly System”, Journal of the American Medical Informatics Association, pp.51-55, 1997.
[3]Isaac S, Kohane, Hongmei Dong, Peter Szolovits, “Health Information Identification and De-Identification Toolkit”, American Medical Informatics Association, 1998.
[4]L. Sweeney, “k-anonymity: a model for protecting privacy”, International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), pp.557-570, 2002.
[5]D. J. Martin, D. Kifer, A. Machanavajjhala, J. Gehrke, and J. Y. Halpern,“Worst-case background knowledge for privacy -preserving data publishing” , In IEEE International Conference on Data Engineering, pp126~135, 2007.
[6] C. Blake and C. Merz. UCI repository of machine learning databases, 1998.