Ataque de reconstrucción de base de datos

Una persona realiza una serie de preguntas a una base de datos para investigar que hay en ella. Son ataques de inferencia para saber que hay dentro de una base de datos que ha sido curada. Utilizando la base de datos curada se trata de obtener datos sobre la base de datos original. Se recomienda evitar tener demasiados detalles en la versión curada.

Preguntas de un adversario

- Una posibilidad es denegar respuestas que podrían ser peligrosas
- El problema es que las denegaciones pueden filtrar información.

Censo ficticio del censo de EEUU

Se construyó una base de datos falsa con 7 personas simulando la del censo. Algunos datos como la edad han sido suprimidos para ciertas personas con el objetivo de proteger contra ataques de inferencia al haber demasiada poca gente cuyos datos como estos coinciden. A pesar de estar estos datos eliminados, se da acceso a datos estadísticos como la media y la mediana, lo que permite ir induciendo poco a poco las edades que han sido ocultadas. Con todo esto se puede proponer un sistema de inecuaciones que se puede aplicar a un algoritmo solver, resultando en que se pueden obtener los datos ocultos de esta forma.