DIFFERENTIAL PRIVACY

Julian Singer and Don Osipov

General Overview

Differential Privacy is the method of concealing sensitive elements of a dataset so that it may be viewed and utilised by outside entities without risking personal information being leaked.

More Overview

Depending on the type of data (i.e. taking a survey, responding to questions, publishing data, etc) different methods may be used. We will cover three of them

Method 1: The LaPlace mechanism

Method 2: The Exponential Mechanism

Method 3: (revealed later)

Adding Noise

When taking a database that we want to protect, rather than just allow access to the real results we can add some “noise”

This means inserting more data as to throw the distribution off, but not by enough as to make it unviable

With all the added noise, one individual’s response does not affect the distribution by much and is thus protected

The weakness to this is that the estimation of the actual data gets more and more accurate as the number of queries to the database increases

Method 1: The LaPlace Mechanism

Usage: query response systems

Purpose: anonymize statistical aggregates like mean

How it works:

- When we have a set of data, it is possible to surmise personal data about individuals from that data when provided with statistics about it
- By adding a set amount of “noise” to the averages of different subgroups, we throw off the accuracy and ability to find individual info without compromising the utility of the data set

Method 2: The Exponential Mechanism

Usage: working with databases

Purpose: publishing an anonymized dataset without infringing on the privacy of the participants

How it works

- Based off of the data set we have, we create a completely new, artificial data set with the same distribution as the original
- A “quality score” is assigned to each output generated by this mechanism based on how likely it is to match the input. Higher scores with higher probabilities are chosen, and used to make the synthetic data set

Method 3: ???

Usage: collecting responses in surveys / gathering user data

Purpose: protecting individuals from the moment data is gathered (large group of participants)

How it works

- ???
- ???

We will try to think through this method together

Example problem

We have 1000 people and we want to ask them if they have a credit score of less than 3. We also want to show the results to the general public without exposing sensitive personal details.

How do we gather accurate data and publish it without risking sensitive personal details being leaked?

Walkthrough of solution

To accomplish this, we conduct our survey as follows:

A person taking the survey flips a coin twice:

If they get heads twice, they answer yes

If they get tails twice, they answer no

If they get any other combination, they answer truthfully

This is an application of the Randomized Response method

Walkthrough continued

To view accurate results of our survey, we simply remove 25% of the yes answers and 25% of the no answers

This is due to the probability that an answer was untruthful being 25% for yes and 25% for no

If we publish our data, there is no way to know if an answer we truthful or forced, but we still get an accurate distribution of the answers

That is how differential privacy works!

Method 3: The Randomized Response

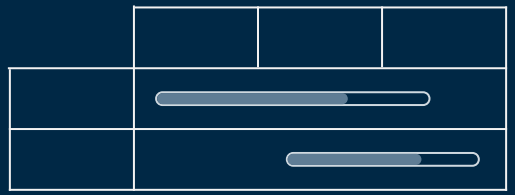
Usage: collecting responses in surveys / gathering user data

Purpose: protecting individuals from the moment data is gathered (large group of participants)

How it works

- When taking a survey, use set parameters to determine if a responder will respond truthfully or give a set response.
- It is possible to determine accurate data that was gathered by accounting for the fixed responses, but impossible to determine individuals responses.

Proof of Concept
/
Code Demo



Practice Problem

You are the CEO of a data analytics company and want to release statistics about a data set you posses on the medical conditions and costs of different families in the US. Design a survey of household medical expenses and conditions and that uses differential privacy to prevent private information from being discoverable.

Additional challenge: After class, try to write a program employing method 2 to further protect the data you collected

Resources

https://www.coursera.org/lecture/security-privacy-big-data-protection/differential-privacy-methods-PyO5J

https://medium.com/georgian-impact-blog/a-brief-introduction-to-differential-privacy-eacf8722283b