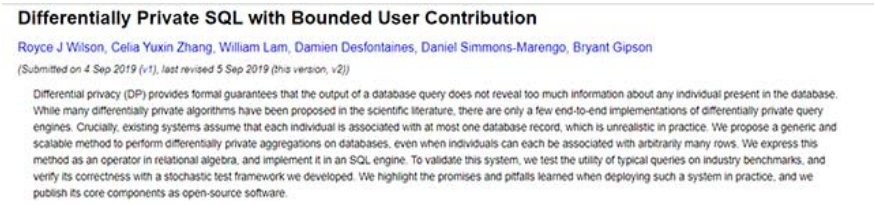
Google released an open source toolkit for companies to enhance the privacy of personal data

Differentially Private SQL is an open source library created to further promote the idea of ??distinct privacy ...

For companies operating in the field of providing services to track online activities of users on the internet, the boundary between respecting or violating the privacy of each individual is always very important. fragile. And a large-scale search and data analysis service provider like Google will undoubtedly be an indispensable link in the problem, or rather, a "mission" to promote respect for privacy in The online world is inherently larger and more complex today.

To achieve that difficult goal, the giant Mountain View decided to build and share an open source library that they use to collect insights from aggregated data in a protected manner. Maximum privacy of each individual.

1. Google released the TensorFlow machine learning framework specifically for graphical data



Differentially Private SQL with Bounded User Contribution

Royce J Wilson, Celia Yuxin Zhang, William Lam, Damien Desfontaines, Daniel Simmons-Marengo, Bryant Gipson

(Submitted on 4 Sep 2019 (v1), last revised 5 Sep 2019 (this version, v2))

Differential privacy (DP) provides formal guarantees that the output of a database query does not reveal too much information about any individual present in the database. While many differentially private algorithms have been proposed in the scientific literature, there are only a few end-to-end implementations of differentially private query engines. Crucially, existing systems assume that each individual is associated with at most one database record, which is unrealistic in practice. We propose a generic and scalable method to perform differentially private aggregations on databases, even when individuals can each be associated with arbitrarily many rows. We express this method as an operator in relational algebra, and implement it in an SQL engine. To validate this system, we test the utility of typical queries on industry benchmarks, and verify its correctness with a stochastic test framework we developed. We highlight the promises and pitfalls learned when deploying such a system in practice, and we publish its core components as open-source software.

Differential Privacy is a statistical technique that ensures privacy in collecting and sharing aggregate information about users

Dubbed Differentially Private SQL, this open source library was created to further promote the idea of ??distinct privacy (DP), a statistical technique that allows for collection and division. share aggregate information about the user - but at the same time ensure privacy.

Basically, this toolkit allows developers as well as construction organizations operating in the field mentioned above to build tools that can learn and filter information from aggregate user data, in when not disclosing any personally identifiable information. Such an approach would be particularly useful in cases where companies want to share confidential data stores with each other without having them leaked or stolen by anonymous attacks.

1. Google updated the error checking feature to draft Gmail, easier to use and smarter

Limit contact and disclose personal information

'If you are a health research specialist, you may want to compare the average amount of time from the time of admission to the discharge of patients in different hospitals to determine if there is any Any significant difference in the way of care as well as the quality of health care services. It is a legitimate and uncommon need in reality. However, if not done properly, the collection and use of this type of data is very easy to violate personal privacy. At this point, Differentially Private will act as an in-depth analytical means, possibly to ensure that all such use of sensitive data is addressed in a way that maximizes the privacy of each personal, " said Miguel Guevara, Product Manager, head of the Google Data Protection and Privacy Office.

1. Google releases an urgent update for Chrome, users should update immediately

Differentially Private will serve as a means of in-depth analysis

If you don't already know, Differentially Private works by adding a random amount of 'noise information' to a personal information file before it is uploaded to the cloud. So basically, data analysis can reveal meaningful and meaningful results while still ensuring that the sensitive data of each individual is not disclosed.

The open source tools shared publicly by Google are basically a process that allows organizations to categorize and analyze different privacy collections on the database. 'In addition to allowing multiple records to be associated with an individual user, system developers can also use these open source tools to calculate quantities, totals, averages, and ratios. percent of analytics data, 'the search giant said.

The main goal of Differentially Private is not to minimize data: It will not prevent companies from finding your personal data. Instead, it helps minimize incidents related to information leakage during sample analysis through data mining techniques.

1. Just finding the security bug is paid by Google, Vietnamese white hat hackers can join

Google is not alone

One of Google's earliest initiatives related to open source tools that support Differentially Private is RAPPOR, a method that helps statistics anonymous data sources from applications like Chrome 'with the ability to guarantee

rights Extremely strong privacy. '

Since then, the company has used this method to protect all the different types of information it has access to, from the location data of Google Fi mobile customers, to the design of features that help determine the popularity of a dish or a restaurant on Google Maps.

The Mountain View company even plans to take advantage of Differentially Private as part of its new proposal on anti-tracking policy for all web platforms, a move that has caused conflicts as well as strong criticism. from cyber privacy advocates.

1. High security but iPhone can still be hacked when accessing malicious websites

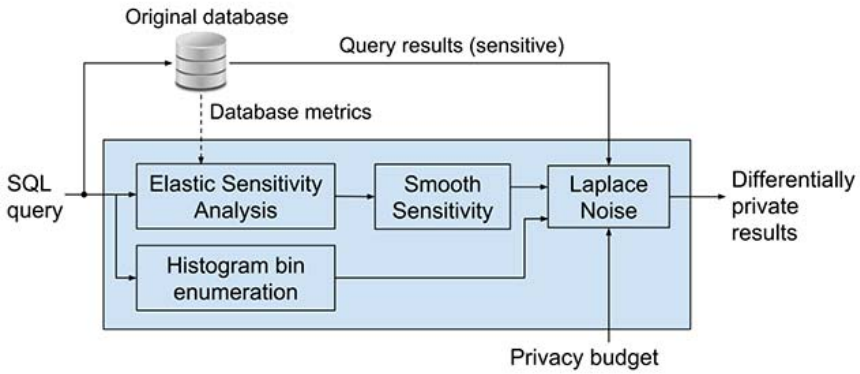
Google can take advantage of Differentially Private as part of its anti-tracking policy proposal for all web platforms

However, Google is not the only name involved in this problem. Differentially Private actually includes all the machine learning algorithms that Apple used to anonymize iPhone user data, while ensuring useful results.

But a 2017 study found flaws in the approach of this approach, especially regarding the 'privacy parameter' - an indicator that helps determine the tradeoff between accuracy. identification and privacy.

Another big business: Uber, also owns a tool similar to Differentially Private called FLEX. This tool has been used to restrict queries that could reveal too much personal information about any Uber driver.

1. Google launched Google Go globally, an extremely lightweight version with many useful features, which can replace the Google app



The Differentially Private model tool is built and deployed by Uber

A large list of open source initiatives

Part of the reason why the Differentially Private deployment diagram is a must and it is not that simple is because it requires a mechanism to ensure safety so that data can be protected from all situations, Unwanted consequences after release, including data breaches.

By turning Differentially Private into an open source tool, Google wants not only to improve its capabilities through extensive feedback from experts, but also from the tech community in general.

Not stopping there, Google also hopes the tool will be more widely accepted by developers without having to design custom Differentially Private solutions.

The open source library announced by Google this time also contains a long list of open source initiatives focusing primarily on privacy, such as Federated Learning, TensorFlow Privacy, Private Join and Compute, Private Set Intersection , and confidential computing . all of which aim to improve privacy and security on different levels in the internet space.

'From medicine, public services, government, to business and beyond, we hope that these open source tools will help create more insights that are beneficial to everyone,' ' Mr. Miguel Guevara said.

1. Chrome will support the HTTP cache partition to prevent malicious attacks and unauthorized tracking

Google is not the only name involved in the privacy issue with Differentially Private

With the current situation of technology majors in Silicon Valley, there is increasing pressure from both state management agencies and public opinion due to a series of painful privacy violations. Google's tireless efforts can be seen as a 'fix', or it can be an effective justification for the collection of personal data for the purpose of revenue-generating advertising business. Application providers, current general service.

In the end, the real benefit of Differentially Private is still something quite vague. However, even if this tool is just a remedy to overcome some of the data security and privacy issues that have been created, it is still worth putting into a deeper application.

You can find out more about Differentially Private at the following addresses:

1. https://github.com/google/differential-privacy/tree/master/differential_privacy
2. https://arxiv.org/abs/1909.01917