Efficient Delegated Private Set Intersection on Outsourced Private Datasets

ABSTRACT

Cloud computing is rapidly gaining in popularity among individuals and businesses, mainly due to the innovation it enables and the opportunities it offers. With its importance increasing, outsourcing datasets and computation to the cloud becomes an appealing approach. Nevertheless, as the cloud cannot be fully trusted the privacy of the outsourced data is a major concern for clients. So, the need arises for protocols that can carry out private set operations on outsourced private data without revealing anything about the data and the computation results to the cloud.

EXISTING SYSTEM

Private set intersection (PSI) is a cryptographic protocol that allows parties to compute the intersection of their datasets without revealing anything about the datasets beyond the intersection. PSI has a range of real-world applications including privacy-preserving data mining, like scenarios where mutually distrusting companies can find out common customers for joint offers without sharing their whole customer data, or ones where social welfare organizations can identify common benefits recipients while protecting the privacy of their beneficiaries; or even homeland security, allowing security agencies to find airline passengers in no-fly lists without having access to the whole passenger list or revealing their no-fly list. Also, PSI can be utilized as a sub-routine in larger privacy-preserving computations such as relationship path discovery in social networks, botnet detection etc. Due to the importance of PSI, researchers have designed numerous PSI protocols. Traditionally, PSI protocols are designed for scenarios in which data owners interact directly with each other using locally stored datasets and jointly compute the set intersection. However, Emergence of cloud computing calls for a change.

Disadvantages

- They do not support outsourcing of the data and the computation to a third party (e.g. the cloud) without non-trivial modifications.

- the parties must re-encrypt their data if they want to compute another intersection, otherwise the cloud can learn even more information about the parties' sets.

PROPOSED SYSTEM

In this paper, we presented two such protocols for private set intersection, O-PSI and EO-PSI. The protocols let clients independently prepare and outsource their private datasets to the cloud. At any point later in time, they can ask the cloud to run PSI on their private datasets. In this process, the cloud learns nothing about the dataset elements, the intersection, and the intersection cardinality. Furthermore, the protocols ensure that the cloud can compute the intersection only when all the clients agree and the clients can securely delegate PSI computation on the outsourced datasets an unlimited number of times with no need to download and re-prepare the datasets. These properties make the protocols particularly suitable for a cloud computing setting, allowing clients to fully benefit from the increased collaboration the cloud enables and the cost-efficient resources it provides without sacrificing their privacy.

Advantages

- Bloom filters, secret sharing and oblivious transfer to offer efficient PSI.
- Using hash tables and a more efficient oblivious transfer extension protocol for better efficiency.

SOFTWARE REQUIREMENTS

Front-end	:	JSP
Back-End	:	MySQL
Server	:	Tomcat Server
OS	:	WINDOWS 7/above

HARDWARE REQUIREMENTS

PROCESSOR	:	CORE i3
RAM	:	512MB-2GB
HARD DISK	:	40GB