Efficient Delegated Private Set Intersection On Outsourced Private Datasets

ABSTRACT

- Private set intersection (PSI) is an essential cryptographic protocol that has many real world applications. As cloud computing power and popularity have been swiftly growing, it is now desirable to leverage the cloud to store private datasets and delegate PSI computation to it.
- Although a set of efficient PSI protocols have been designed, none support outsourcing of the datasets and the computation.
- In this paper, we propose two protocols for delegated PSI computation on outsourced private datasets

CONT

- Our protocols have a unique combination of properties that make them particularly appealing for a cloud computing setting. Our first protocol, O-PSI, satisfies these properties by using additive homomorphic encryption and point-value polynomial representation of a set.
- Our second protocol, EO-PSI, is mainly based on a hash table and point-value polynomial representation and it does not require public key encryption; meanwhile, it retains all the desirable properties and is much more efficient than the first one.
- We also provide a formal security analysis of the two protocols in the semi-honest model and we analyze their performance utilizing prototype implementations we have developed.

Existing System

- Cloud computing offers flexible and cost effective storage and computation resources to clients and has been attracting the attention of individuals and businesses as a vital enablingtechnology
- A report by the IBM Institute for Business Value in 2012found that cloud computing is driving business innovationalong a number of dimensions, with its ability to enable increasedcollaboration with external partners and its cost advantages as themost important objectives for business adoption.

Cont

- Organizationshave been keen to adopt cloud computing in order to reap thebenefits it promises. A 2016 RightScale report found that 95% of organizations surveyed are running applications or experimenting with the cloud. In general, "surveys show that more than half of all enterprises consider the cloud to be an essential part of their business models and are willing to devote 50% or more of their IT budget to the cloud"

DISADVANTAGES

- The cloud cannot be fully trusted the privacy of the outsourced data is a major concern for clients.

Proposed System

- In this paper, we present two protocols for delegated PSI onoutsourced private datasets. Our first protocol, O-PSI, is basedon additive homomorphic encryption and point-value set representation.
- The protocol lets clients independently outsource theirdatasets by representing them as blinded polynomials.
- To achievedelegated PSI computation, homomorphic encryption is used to“switch” blinding factors so that the outsourced datasets blindedunder different blinding keys can now be combined in the compu-tation process.

Cont

- The protocol ensures that intersections can only becomputed with the permission of all the clients and that the result(i.e. the intersection and its cardinality) will be protected from thecloud. The protocol also allows the datasets to be used securely anunlimited number of times without the need to secure them again.Although O-PSI has all the desirable properties, it is somewhatinefficient, as it requires costly homomorphic encryption (opera-tions) which has a major impact on its performance.

Advantages

- Its importance increasing, outsourcing datasets and computation to the cloud becomes an appealing approach

HARDWARE REQUIREMENTS

System	: Pentium IV 2.4 GHz.
Hard Disk	: 40 GB.
Floppy Drive	: 1.44 Mb.
Monitor	: 15 VGA Colour.
Mouse	: Logitech.
Ram	: 512 Mb.

SOFTWARE REQUIREMENTS

Operating system	: Windows XP/7.
Coding Language	: ASP.net, C#.net /java

Conclusion

- 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.In this paper, we presented two such protocols for privateset intersection, O-PSI and EO-PSI. The protocols let clients independently prepare and outsource their private datasets to the cloud.