Literature Survey on Secure Multiparty Anonymous Data Sharing

Reshma Scaria[1*] Lekshmi Priya S[2] Sushitha Susan Joseph[3]

1. Student, Department of CSE, Mar Baselious Christian College of Engineering and Technology, Kuttikanam, Peermade, Kerala, India.
2. Student, Department of CSE, Mar Baselious Christian College of Engineering and Technology, Kuttikanam, Peermade, Kerala, India.
3. Assistant Professor, Department of CSE, Mar Baselious Christian College of Engineering and Technology, Kuttikanam, Peermade, Kerala, India.

*reshmascaria93@gmail.com

Abstract

The popularity of internet as a communication medium whether for personal or business requires anonymous communication in various ways. Businesses also have legitimate reasons to make communication anonymous and avoid the consequences of identity revelation. The problem of sharing privately held data so that the individuals who are the subjects of the data cannot be identified has been researched extensively. Researchers have understood the need of anonymity in various application domains: patient medical records, electronic voting, e-mail, social networking, etc.

Another form of anonymity, as used in secure multiparty computation, allows multiple parties on a network to jointly carry out a global computation that depends on data from each party while the data held by each party remains unknown to the other parties. The secure computation function widely used is secure sum that allows parties to compute the sum of their individual inputs without mentioning the inputs to one another. This function helps to characterize the complexities of the secure multiparty computation.

Keywords: Anonymity,Secure multiparty computation

1.Introduction:

Multiparty data sharing deals with how we can secure multiparty data sharing. There are efficient algorithms for assigning identifiers (IDs) to the nodes of a network such that the IDs are anonymous by using a distributed computation with no central authority. In order to have complex secure data sharing AIDA can be used so that the computation will be easier than the existed one. The main algorithm is based on a technique for anonymously sharing simple data and results in methods for efficient sharing of complex data.

There are many applications that require dynamically generated unique IDs for network nodes. Such IDs can be used as part of schemes for sharing/dividing communications bandwidth, data storage, and many other resources without conflict. An application where IDs need to be anonymous is mainly grid computing where one may seek services without exposing the identity of the service requestor.

This paper presents a survey on various papers based on the data sharing with anonymous IDs that were proposed earlier. Also, this paper provides a marginal overview for future research and improvements.

2. Literature Review

In [1], the authors propose a two-argument function is computed privately by two parties such that after the computation, no party should know anything about the other inputs except for what he is able to calculate from his own input and the function value. Some general relations between the information gain of an optimal protocol and the communication complexity of a function is also mentioned. In this paper, measures for revealed information required for computing *f* have been considered. Mainly analyzed the measures given by Bar-Yehuda and have also showed that some results presented by them are wrong on two-party computation. They have introduced a new definition for the additional information for two party protocols and have given some bounds for concrete functions for the additional information. Here they have made use of calculations which are difficult.

In [2], they are discussing about Secure Multi-Party Computation(SMC). Secure Multi-Party Computation (SMC), is a technique that allows parties with similar background to compute results upon their private data, minimizing the threat of disclosure. The exponential increase in sensitive data which needs to be passed upon networked computers and the growth of internet has developed vast opportunities for cooperative computation, where parties come together to facilitate computations and draw out conclusions that are mutually beneficial and at the same time helps to keep their private data secure. This paper is mainly an extension to a previously proposed protocol Encrytpo_Random, which presented a simple but effective approach to SMC and also put forward an suitably developed architecture, whereby such an efficient protocol, involving the parties that have come forward for joint computations and the third party who undertakes such computations, can be developed. Through this extended work an attempt has been made to further strengthen the existing protocol and makes use of several layers in architecture. These layers are making the whole system greatly confusing.

For assigning identifiers to the nodes of a network, efficient algorithms are dealt such that the identifiers are anonymous by making use of a distributed computation devoid of central authority. In [3], the secure sum allows parties to work out the sum of their individual inputs devoid of disclosing the inputs to each another and it helps to differentiate the complications of the secure multiparty computation. An algorithm was presented for sharing simple integer information on top of secure sum and it is used by the algorithm at all iterations for anonymous ID assignment. But the secure sum does not allow to share complex messages.

A secure computation function widely used in the literature of [4], which is secure sum that allows parties to compute the sum of their individual inputs without disclosing the inputs to one another. This function is popular in data mining applications and also helps explain the complexities of the secure multiparty computation. To differentiate anonymous ID assignment from anonymous communication, consider a situation where parties wish to display their data collectively, but anonymously, in slots on a third party site. The IDs can be used to assign the slots to users, while anonymous communication can allow the parties to conceal their identities from the third party. While looking it more closely its clear can that the data being shared in wireless networks is not quite easy.

In [5], the perturbation approach and the k-anonymity model are two major techniques for privacy-preserving. The k-anonymity model assumes a quasi-identifier (QID), which is a set of attributes that may serve as an identifier in the data set. In the simplest case, it is assumed that the dataset is a table and that each tuple corresponds to an individual. But the privacy may be violated if some quasi-identifier values are unique in the released table.

The [6], deals with efficient algorithms for assigning identifiers (IDs) to the nodes of a network in such a way that the IDs are anonymous that is randomly generated using a distributed computation with no central authority. Given N nodes, this assignment is essentially a permutation of the integers {1,…,N} with each ID being known only to the node to which it is assigned. The main algorithm is based on a method for anonymously sharing simple data and results in methods for efficient sharing of complex data. So this algorithm requires solving a polynomial with coefficients taken from a finite field of integers modulo a prime. That task restricts the level to which can be practically raised.

In [7], an algorithm for sharing simple integer data on top of secure sum is built. The sharing algorithm will be used at each iteration of the algorithm for anonymous ID assignment (AIDA). This AIDA algorithm, can require a variable and unbounded number of iterations. By using the Newton identities greatly decreases communication overhead. This can enable the use of a larger number of “slots” with a consequent reduction in the number of rounds required. The solution of a polynomial can be avoided at some expense by using Sturm’s theorem. With private communication channels, this algorithm is secure in an information theoretic sense. In contrast to bounds on completion time developed in previous works, the formulae give the expected completion time exactly.

3.Conclusion

This paper presents a survey on various techniques and algorithms that was proposed earlier by researchers for the better privacy-preserving data access. The proposed AIDA algorithm is foolproof in allocating ID to users and the anonymous identity is maintained, thus providing ample proof for the sets of users in multiparty environments. Even under difficult situations the communications and bandwidth is not affected in any manner. So unlike cryptographic measures and traditional systems AIDA proves to be secure for distributed architecture keeping the user safe from attacks in different segments. In future the scheme may be extended as a web service so that any interconnected user of the network can utilize it to the maximum without the need to implement the code. Also mobile web services are an area of interest for future extensions to AIDA.

References

[1] Andreas Jakoby and Maciej Li´skiewicz (2005), "Revealing Additional Information in Two-Party Computations " , Advances in Cryptology - ASIACRYPT 2005 Lecture Notes in Computer Science Volume 3788, 121-135.
[2] Dr. Durgesh Kumar, Neha Koria, Nikhil Kapoor, Ravish Bahety (2009), "A Secure Multi-Party Computation Protocol for Malicious Computation Prevention for Preserving Privacy ..During Data Mining", International Journal of Computer Science and Information Security,Vol. 3.
[3]Akheel Mohammed, Sajjad Ahmed Md , Ayesha (2013), "Confidentiality And Anonymity Strengthening in Computational Services", IJRRECS,Volume-1,Issue-6,1006-1011.

[4]Swathi, P.Jyothi, and Anil Kumar(2014), "Assigning Privacy Ids For Each Data That Have Been Sharing In Wireless Networks", International Journal of Communication Network and Security (IJCNS) ISSN: Volume-2, Issue-3.

[5] Ms. R. Kalaivani, Ms. R. Kiruthika (2014), "Automated Anonymous Id Assignment For Maintaining Data Privacy", International Conference on Science,Engineering and Management,Srinivasan Engineering College, India.
[6] Ayswarya R Kurup, Simi Lukose (2014), "Security Enhanced Privacy Preserving Data sharing With Random ID Generation",IJSRE Volume 2 Issue 8.
[7] Larry A. Dunning, And Ray Kresman (2013), "Privacy Preserving Data Sharing With Anonymous ID Assignment ",IEEE Transactions on Information Forensics and Security, Vol. 8, NO. 2.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar