IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 04, Issue 09 (September. 2014), ||V4|| PP 48-51

Confidential Multiparty Computation with Anonymous ID Assignment using Central Authority

P Babitha[1], K R Lavanya[2]
[1]*Assist Professor, Siddartha Institute of Science and Technology, Puttur,*
[2]*Assist Professor, Siddartha Institute of Science and Technology, Puttur,*

Abstract- For giving out private data securely between several parties an algorithm has been used. An anonymous ID assignment technique is used iteratively to assign the nodes with ID numbers ranging from 1 to N. This technique enhances data that are more complex to be shared securely. The nodes are assigned with the anonymous ID with the help of a central authority. The algorithm has been compared with the existing algorithm. In this paper we propose an algorithm has been developed based on Sturm's theorem and Newton's identities. The numbers of iterations are found out with the help of Markov chain.

Keywords:- *Anonymous Id,* ***AIDA****-Anonymous Id Assignment.*

I. INTRODUCTION

The anonymous message plays a very significant role in internet's popularity for both individual and for the purpose of business. Cloud based website management tools enable the servers to analyze the user's behavior. The disadvantages of giving out private data are being studied in detail. Other applications for anonymity are various viz electronic voting, social networking, Doctor medical records, and many more. In secure multiparty computation which is a new form of anonymity allows several multiple parties to share data that remains unknown? A secure computation function enables multi parties to compute the sum of their inputs rather than revealing the data. This method is very much well-liked in data mining operations and enables classifying the complexities of secure multiparty computation.

Our main algorithm is built on top of a method that shares simple data anonymously and yields a technique that enables sharing of complex data anonymously. With the help of permutation methods the assigned ID are known only to the nodes which are being assigned IDs. There are several applications where network nodes needs self-motivated unique IDs. One such application is grid computing where the services are requested without disclosing the identities of the service requestor. To differentiate between anonymous communication and anonymous ID assignment, think about a situation where N parties wish to exhibit their data in total, in N slots on a third party site, anonymous ID assignment method assigns N slots to the users whereas anonymous communication allows the users to conceal their identities In our network the identities of the parties are known but not the true identity. In this project we use an algorithm for sharing simple integer data which is based on secure sum. This algorithm is used in every iteration of anonymous ID assignment. Here we consider all the nodes to be half direct. Even though they follow a set of rules for message if they happen to see information they might intrude.

In existing system, the information about each node will be shared along with the data. It is usually encrypted along with the data. Newton's polynomial usage cannot be avoided as it increases the number of rounds of iterations that are used to compute the secure sum and power sum. Hence the performance of the system also becomes low. Sum inputs are only focused whereas our project deals with the number of rounds. Secure multiparty computation usage is being avoided with the usage of Sturm's theorem to make sure that the information about the nodes are not revealed. In the current system the main goal is to provide anonymous id for each node. Each node will have a secure communication of simple and complex data. These data's may be from static or dynamic data. By implementing secure sum hides permutations method and anonymous id assignment (AIDA) method the permutation methods are kept anonymous to each other. Hence here encoding technology is used to create anonymous ID and the ID is being assigned to the user by the central authority and the receiver receives the data and decodes it with the key that is known only to the sender and the receiver which might not be known to the other semi honest node that might intrude.

II. MODULES DESCRIPTIONS

AUTHENTICATION

The process of identifying an individual usually based on a username and password. In security systems, Authentication merely ensures that the individual is who he or she demands, but says nothing about the access rights of the individual.

1 LOGIN:

In User and Admin login we are going to check whether the system is trusted machine or distrust machine. If the machine is trusted then the user or admin is allowed with n attempts. If the machine is distrusted machine then the user is allowed with single attempt. Process Involved is to Check the login name and password Then allows the authorized user to use these pages. If the unauthorized user attempts to access user login then restrict that user and give the information.

A FORGETS PASSWORD:

When the users forget their password then the user can access this forget password. It can be used to create a new password. To make sure that user accessing forget password is a legitimate user, the user will be asked a question. Then the questions and their answers are created, while the user is registering to the site. If the user enters the answer then the entered text will be matched with the database. If the result is true, then the user will be allowed to enter the new password to access the site. If the result is false, user will not be allowed to enter the new password to access the site.

B REGISTRATION:

When a new user is creating an account he needs to register here by giving the sufficient information. Registration might also contain some private data that will be kept confidential so that the information about username and password is retrieved when it is forgotten.

2 ADMIN:

In this module when the admin attempts to login we need to find whether the machine is trusted or it is suspected machine and it is found by user id and password. Admin can facilitate to all nodes. With the help of that AID each node can share the data in internet. Admin can generate that facility for individual nodes. So the sharable data can be kept in a sharable database. As a result their own private data will be maintained secret.

A GENERATES AID:

In this module admin wants to create the AID for individual nodes and admin can make this unique AID for each user presented in network. With the help of this AID user can share his data and also he can keep his own private data as secret.

B ASSIGN AID:

Admin can provide unique AID to all nodes. Nodes presented in network will be communicating by using AID. AID can not contain any private information.AID helps to keep personal information as more secret.

III. USERS

Users can login by entering the given username and password. Then he/she may go for corresponding page. User can keep his own information in a sharable data base. And also he can retrieve data shared by other users. User has to use his AID for sharing information.

A SHARE DATA:

New user has to get AID from admin. Admin will assign that AID for every node. So data shared by user can be kept in a sharable database and it can be shared by all users. Each node will have unique AID with the help of that unique AID any user can store and retrieve from sharable database.

B RETRIEVE SHARED DATA:

In this module user can retrieve the shared data. Shared data may be stored by him or by any other node. So it will be easy to make own private data as secret by implementing anonymous id algorithm.

A SHARE DATA:

New user has to get AID from admin. Admin will assign that AID for every node. So data shared by user can be kept in a sharable database and it can be shared by all users. Each node will have unique AID with the help of that unique AID any user can store and retrieve from sharable database.

B RETRIEVE SHARED DATA:

In this module user can retrieve the shared data. Shared data may be stored by him or by any other node. So it will be easy to make own private data as secret by implementing anonymous id algorithm.

Secure sum Algorithm

Given nodes each holding an data item from a finitely represent able abelian group, share the value among the nodes without revealing the values .

1) Each node, chooses random values such that

ri,1+…ri,N = di

2) Each "random" value is transmitted from node to node . The sum of all these random numbers is, ofcourse, the desired total .

3) Each node totals all the random values received as:

si,j = r1,j+…+ rN,j

4) Now each node simply broadcasts to all other nodes so that each node can compute:

T = s1 +…sN

AIDA Algorithm Implementation:

Given nodes n1,…,nN, use distributed computation (without central authority) to find an anonymous indexing permutation s : {1,…,N} {1,…,N}.

1) Set the number of assigned nodes A = 0.

2) Each unassigned node chooses a random number in the range 1 to S. A node assigned in a previous round chooses r1 = 0.

3) The random numbers are shared anonymously. Denote the shared values by q1,…,qN.

4) Let q1,…,qk denote a revised list of shared values with duplicated and zero values entirely removed where k is the number of unique random values. The nodes ni which drew unique random numbers then determine their index si from the position of their random number in the revised list as it would appear after being sorted: si = A + Card{qj : qj <=ri}

5) Update the number of nodes assigned: .

6) If A < N then return to step (2).

Basic formula

P (collision) =1-e^(-N^2/(2*H))=alpha

N=sqrt (2*ln (1/1-alpha))*sqrt (H)

N: number of evenly distributed hashes to compare

H: the Size of the element count of all possible hashes

H=2^ (IDlength *ln (36)/ln (2))

Hashes calculated with SHAI (IDlength<=30). K.Communications Requirements of AIDA Methods Consider the required number of data bits for each of the three variant methods just described. This is the number of data bits that would be transmitted in each packet by the secure sum algorithm introduced earlier. The required numbers of data bits B are slightly overestimated by the formulae: $Bprime$ = N. [$log2$(P+1)] $Bprime$ = N. [$log2$(N)] /2.[$log2$(S)] $Bprime$ = S. [$log2$(N+1)] (2) The computational requirements of the "slot selection" appear, at first, to be trivial. However, for every root that the "prime modulus" method must check, "slot selection". *L. The Completion Rate after R Rounds* Two nodes might make identical choices of random numbers, or slots as they will be termed in this section. One can only guarantee that a complete assignment of nodes using possibilities for slots or random number choices and rounds will occur with at least a desired probability. The formulae are derived by assuming that N -1 node have chosen slots and looking at the next choice. The Nth node into choose a slot resulting in assignments and conflicts. The slot it chooses could be unassigned, already in conflict with multiple occupants, or already assigned with exactly one occupant.

III. EXPERIMENTAL RESULTS

SI.NO	N	H	P
1	189	45	390
2	210	55	400
3	290	95	442
4	549	225	667
5	999	455	1109

Table 1: Anonymous ID creation Algorithm

Results are given in terms of identities. N represents the number of evenly distributed hashes to compare. H indicates the size of the element count of all possible hashes. P Indicates the value of anonymous

ID. This is unique to every members of the group. Anonymous ID received is unknown to other members of the group. Anonymous id is examined between communication and computational requirement.

IV. CONCLUSION

Proposed paper greatly decreases communication overhead. By using private communication channel that is anonymity router to transmit the data more securely. To overcome the problem of identifying details and changing information anonymous id was utilized. Random serial number is used to identify whether the data requesting person is a correct authorized person or hackers. The use of 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. The development of a result similar to the Sturm's method over a finite field is an enticing possibility. With private communication channels, the algorithms are secure in an information theoretic sense. Apparently, this property is very fragile. The very similar problem of mental poker was shown to have no such solution with two players and three cards. The argument can easily be extended to, e.g., two sets each of N colluding players with a deck of 2N+1 cards rather than our deck of 2N cards. In contrast to bounds on completion time developed in previous works, our formulae give the expected completion time exactly. All of the no cryptographic algorithms have been extensively simulated, and the present work does offer a basis upon which implementations can be constructed. The communications requirements of the algorithms depend heavily on the underlying implementation of the chosen secure sum algorithm. In some cases, merging the two layers could result in reduced overhead.

REFERENCES

[1]. Sarbanes–Oxley Act of 2002, Title 29, Code of Federal Regulations,Part 1980, 2003.

[2]. Y.Zhang, W.Liu, and W.Lou .Anonymous communications in mobile ad hoc networks. In INFOCOM 2005, 24th annual joint conference the IEEE Computer Societies. Proceeding IEEE, volume 3, pages 1940– 1951, March 2005.

[3]. D. Chaum, "Untraceable electronic mail, return address and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–88, Feb.1981.

[4]. C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, and M. Y. Zhu, "Tools for privacy preserving distributed data mining," ACM SIGKDD Explorations Newsletter, vol. 4, no. 2, pp. 28–34, Dec. 2002.

[5]. J. Wang, T. Fukasama, S. Urabe, and T.Takata, "A collusion-resistant approach to privacy-preserving distributed data mining," IEICE Trans.Inf.Syst. (Inst. Electron. Inf. Commun. Eng.), vol. E89-D, no. 11, pp.2739–2747, 2006.

[6]. F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi, and A.Vaccarelli, "Seas, a secure e-voting protocol: Design and implementation," Comput. Security, vol. 24, no. 8, pp. 642–652, Nov. 2005.

[7]. Sanil, A. P., Karr, A. F., Lin, X., and Reiter, J. P. (2007). Privacy preserving analysis of vertically partitioned data using secure matrix products.

[8]. J. Kong and X. Hong. Anodr: anonymous on demand routing with untraceable routes for mobile ad-hoc networks. InMobihoc'03: Proceedings of the 4th ACM international symposium on Mobile ad hoc networking ages 291–302, New York, NY, USA,2003.

[9]. J. Yoon and H. Kim, "A new collision-free pseudonym scheme in mobile ad hoc networks,"5th workshop on Resource allocation, Cooperation and competition in wireless networks. June 2009.

[10]. A. Friedman, R. Wolff, and A. Schuster, "Providing k-anonymity in data mining," VLDB Journal, vol. 17, no. 4, pp. 789–804, Jul. 2008.

[11]. J. Domingo-Ferrer, "A new privacy homomorphism and applications," Information Processing Letters, vol. 60, no. 5, pp. 277–282, December1996.[Online]. Available: citeseer.nj.nec.com/290190.html

[12]. J. Domingo-Ferrer, "A provably secure additive and multiplicative privacy homo morphishm," in Information Security, ser. Lecture Notes in Computer Science, A. Chan and V. Gligor, Eds., vol. 2433. Springer Verlag, 2002, pp. pp. 471–483.

[13]. D. M. Goldschlag,M. G. Reed, and P. F. Syverson, "Hiding routing information," inProc. Information Hiding, 1996, pp. 137150,Springer Verlag

[14]. A. Karr, "Secure statistical analysis of distributed databases, emphasizing what we don't know," J. Privacy Confidentiality, vol. 1, no.2,pp. 197–211, 2009.

[15]. Q. Xie and U. Hengartner, "Privacy-preserving matchmaking for mobile social networking secure against malicious users," in Proc. 9thAnn. IEEE Conf. Privacy, Security and Trust, Jul. 2011, pp. 252–259.