Securely Data Sharing with Indeterminate ID Allocation

V. Lasya [1], M. Prasanthi [2], Abdul Vahed [3]

[1] *pursuing M.Tech (CSE) from Sri Sunflower College of Engineering and Technology, challapalli, Krishna (D) , Andhra Pradesh 521131 India*

[2] *working as Assistant Professor(CSE) from Sri Sunflower College of Engineering and Technology, challapalli, Krishna (D), Andhra Pradesh 521131 India*

[3] *working as Associate Professor & HOD(CSE) from Sri Sunflower College of Engineering and Technology, challapalli, Krishna (D), Andhra Pradesh 521131 India*

Abstract: We are introducing a novel algorithm for anonymous data sharing of private data from different persons. By using this mechanism we are assigning nodes ID number from 1 to N. This assignment is anonymous in that the individuality receives the information without knowing identity of this to other member of in the group. Prevent to collision from other members in the theoretic sense whenever they are using private communication channel. This serial numbers assignment allows the user to share most complex data and contains the applications of other problems in the data mining, Remove collision when they are communicating and circulated database access. Here the necessary computation is distributed instead of central authority.

The current and new approaches for allocating anonymous IDs are examine with respect to trade-offs between communication and computational necessity. The new algorithms are design secure mining algorithms using sturm's and newton's theory. Markov chain representation is used to statics on number of iterations needs, and the computer algebra gives the complete closed form results on completion rates.

Keywords:-Anonymous assignment, private communication channel, trade-offs, privacy protection

1. INTRODUCTION

Nowadays the internet usage became very popular as communication media, this is using for sharing personal and business related data with anonymous user, and the business related data also engaged in communication without disclosing the identity of actual person. For adopt there is requirement to dispense summery of data without revealing identity of person and the corresponding data is associated with electronic or political revenge 1) cloud based website management 2) and providing some capacity to maintain user actins on browser for protecting data 3) The investigators also research of related anonymity and privacy with other domains like medical records of patients 4) email 5) electronic voting 6) social networking.

Other side of anonymity, which is used in multipart computation, which means the different parties jointly carry global computation on network depends on the data each party, that held on each part unknown to each other. In this article we are providing secure some for individuals. This allows the parties compute their sum of input without revealing input of each other. This function is useful in data mining application and also categorized the difficulty of secure multipart data.

This work is useful to efficient algorithms for providing IDs to nodes on network in such that the nodes are anonymous using distributed computation with no central authority. Given N nodes the permutations of integers{1,….N} each ID being known only to the nodes which is assigned. Our algorithms are based on method simple data sharing anonymously and the results for the methods efficiently sharing complex data. Many applications require dynamic IDs in the network, such IDs using as part of sharing, communication, data storage, band width, and some other resources without any clash. These IDs are desired in sensor networks to provide some security or some administrative tasks for reliability, that is configuration and monitoring, and download for data aggregation or binary code for these nodes.

To divide the anonymous ID segmentation from anonymous communication, here were taking a situation, where all N parties want to display their data uniformly, by anonymously, in N slots on third party site. The ID are allocated to users, while performing anonymous communication, this able to allows the parties to hide their information with Third party.

The work in this paper exposes the connection between sharing sensitive information in anonymous manner, allocate

multipart computation secrecy and the anonymous ID allocation. The word meaning anonymous is different for research is symmetric access election leader in network. Here our network is not anonymous the identity of parties is revealed each while they are communicating.

The methods allocated and used for set of aliases, have been introduced for anonymous communication in mobile networks. Our network needs a trusted administrator, as declared, and their end products totally different with our to form statistical properties. To be detailed, by nodes the procedures of this article allocate a calculation between the nodes producing a variation of chosen with an unchanging prospect of from set of all variations of where will know only. Such a variation can also be generated by algorithms designed to mental poker. The algorithms which are developed for mental poker are big complex and use cryptographic techniques as the players 'necessity, in general, to capable to demonstrate that they apprehended the winning hand. Total complete in this paper, we think that the members are *semi honest*, it is also identified as inactive or honest-but-curious, and perform their compulsory protocols devotedly. We are given a reliable, semi-honest, and trusted third-party, a variation could also be made by using an anonymous routing protocol. Regardless of the differences quoted, the reader must contact and deliberate other algorithms stated above before executing the algorithms in this paper.

In this article we are design an algorithm for accessing humble numeral data on secure sum. For anonymous ID assignment (AIDA) the utilization of sharing algorithm in every repetition of an algorithm. This AIDA algorithm, and the variations that we are discussed, can be requiring an inconstant and boundless number of iterations. The finite restricted algorithms for AIDA will be discussed further. Parameter increasing in this algorithm will be decrease the number of predictable rounds. Though, the proposal central algorithm requires resolving a polynomial with quantities taken from a limited field of numeral modulo a major. That work controls the level to which can be practically elevated. We are representing in detail how to inherit the average number of necessary rounds, and in the Adjunct detail a technique for resolving the polynomial, which can be dispersed among the users who are participated.

2. A REVIEW OF SECURE SUM

Assume that a set of hospitals with different databases want to calculate and share only the mean of a data item instead of total, such as number of hospitals need contagions, without disclosing the value of this hospital data item for any person of this group. Thus, the data items d1,d2,d3,….d_n contained by nodes $n_1,n_2,n_3,….N_n$ and want to compute and share only data value $T = d_1+d_2+d_3+….d_N$. A protected sum algorithm permits the sum to be together with some assurances of secrecy. Again, we adopt the semi-honest idea of confidentiality conserving data mining. Under this technique, every node should follow the protocol rules, but might be use any other information it realizes during the implementation of the compromise security protocol.

Would altogether pairs of nodes have a secure communication channel available; a simple, but source rigorous, secure sum algorithm can be built. In the bellowalgorithm, it is beneficial to understand the values as being integer in the first reading:

TABLE I

The secure some execution Random numbers transmitted

Nodes	$\hat{r}_{i,1}r_{i,1}$	$r_{i,2}$	$r_{i,3}r_{i,4}d_id_i$			
$n_{i=1}$:	13-6+8=15	13	-10	6	-3	6	8
$n_{i=2}$:	7-10+9= 6	73-5510	9				
$n_{i=3}$:	-8-6+5=-9	-8	1112	-9	6	5	
$n_{i=4}$:	66-8-592	2					
$s_{i=}$	18	18	-4	8	2	T=24	24

Algorithm I (Secure sum): The nodes n_1, n_2…N_n, contains data items on individual di, from a finite set. Share the value $T = \sum di$ between the nodes without disclosing the d_i values.

1) Every node n_i, i = 1,….Nselect random generated values $r_{i,1},…r_{i,N}$ such that

$r_{i,1}+…..r_{i,N} = d_i$

2) Each and every random value $r_{i,j}$ is conveyed from n_i node to n_j node, some of all these random numbers $r_{i,j}$ is wanted total T
3) All the values received to each node received as:

$S_j = r_{1,j} + r_{N,j}$

4) To all other nodes broadcast s_i by all other nodes so that each node can compute.

$T=s_1+…s_N$

4. USING POWER SUMS TRANSMITING SIMPLE DATA

Supposethat all of our set of nodes wants to share actual data values from their data bases instead of depends on statistical information as described in the previous session. That is each node n_i of a group of N no of nodes n|[N] contains a data item d_i which is used to

communicated with in the same group. We are introducing collusion resistant approach using secure sum mechanism it treated as original communication technique. In this technique our data items d_i are taken from finite field F, in the general case each every di treated as integer values and the field F where p is treated as prime number satisfying the $P>d_i$ for all i. Like the arithmetic will be perform typically using p module, but here other fields also to be used.

Algorithm 2(Anonymous data sharing with power sums):
All the given nodes n_1, n_2, … n_N contains data items d_i from finitely represent table field F, make their data items to public to all the nodes which are available in the group.

1) Every node n_i calculate $d^n{}_i$on the field F for n = 1,2,…N, then the nodes use the power sum to share knowledge.

$P1 = \sum_{i=1}^{n} d_i^1$	$P1 = \sum_{i=1}^{n} d_i^1$	….	$P1 = \sum_{i=1}^{n} d_i^1$

2) Power sum P_1,…..,P_N these are used to produce the polynomials which contains data items d_i,…,$d_N$as its roots by using Newton's identities.
The polynomials are represented as bellow

$$P(X) = CNX^N + \cdots + C_1X + 0$$

The values C_0, to C_N get from the equation
C_N = -1
$C_{N-1} = -\frac{1}{1}(CNP_1)$
$C_{N-2} = -\frac{1}{2}(C_{N-1}P_1 + C_NP_2)$
$C_{N-3} = -\frac{1}{3}(C_{N-2}P_1 + C_{N-1}P_2 + C_NP_3)$
$C_{N-4} = -\frac{1}{4}((C_{N-3}P_1 + C_{N-2}P_2 + C_{N-1}P_3 + C_NP_4)$
$C_{N-m} = -\frac{1}{m}\sum_{k=1}^{m} C_{N-m+k}\,P_k$

3) The polynomial P(x) is resolved by every node, or doing by computation distributed between node, determined by d_1, ..d_N.
The power sum could be gathered or shared by using a single secure sum by sending a request in the array by applying methods to a vector conveying and get. Power sums are symmetric type of methods, so there is no association is did between n_i and the value of d_i. Though, the information consist in sum is used to find the data item value d_1, …, d_N.

TABLE II
Powers of data values di, chosen by each node Module p=11

d_i^e	e=2	e=3	e=4e=5
$n_{i=2}$:	7	37	9
$n_{i=3}$:	10	110	1
$n_{i=4}$:	7	37	9
$n_{i=5}$:	2	38	5
$\sum d_i^e$	p1=2	p2=0	p3=10 p4=10

All the nodes which receive values P_1, P_2, P_3, and $P_4$and will compute it routes and the polynomial to recover its original data items but not theirs indices.

3. SHARING COMPLEX DATA WITH AIDA

Now deliberate the probability of complex data sharing with in the participating nodes n_i which contains the data item d_i are wishing to public namelessly to other contributors.
The number of bits per data items and participants in the group is become larger, the mechanic of prior session is made as infeasible, rather to accomplish this task, we will use the nodes index, the techniques to identify the indexing developing in further sections. Think that every node n_i contains ID or a serial number s_i = {1,2,…N}, further no one node has idea about ID number and si another nodes, further s_1,….s_N has random variation for 1,…N. This again called as Anonymous ID Assignment (AIDA).
This AIDAs are used to allocate slots with respect to time and storage space for communication. It might be simply for central storage location C $_i$, have their databases, so every node stores the data with setting C_i:=di.

4. HOW TO FIND AN AIDA

Here we introducing a simple algorithm to find an AIDA which has numerous different dependencies, on the option of data accessing, for that we are mentioned 3 steps below. In the first step the integer or slots between 1 to S are selected by every node. Based on defining slots the nodes position will be disclosed, but here facility must be created for collusion. The limitation S has been taken as S ≥ N

R	Step	A	r1 r2 r3 r4	r1 r2 r3 r4	s1 s2 s3 s4
1	2	0	6 10 6 2	6 10 6 2	
1	3	0	6 10 6 2	2 6 6 10	
1	4	0	6 10 6 2	2 10	2 1
1	5	2			2 1
2	2	2	5 0 6 0		2 1
2	3	2	5 0 6 0	0 0 5 6	2 1
2	4	2	5 0 6 0	5 6	3 2 4 1

Algorithm: In this algorithm we will find AIDA, for that taken nodes $n_1,\ldots n_N$, using distributed computation to identify the permutation of anonymous indexing s : {1,…,N} →{1,…,N}

1) Arrange the number for assigned nodes A = 0.
2) Every unassigned node n_i will select a random number ri in the range between 1 to S.
3) The random numbers are anonymously share. A method is described for this operation. Denoting shared values $q_1,\ldots q_N$.
4) Let q1,… qk denoted the shared values, the duplicate and zero was completely remove, where k is the unique random shared value. The nodes n_i explain the numbers in distinctive mode after That define their indexing s_i from the position in the list the revised values after sorting.

$$Si = A+Card\{q_j:q_j< = r_i\}$$

5) After that need to update the number of values assigned A = A + K

Example: (Execution of an algorithm for finding an AIDA): Assume4 nodes are participating in finding AIDA, To make simple we continue our example with s = 10 and the random number choices 6,10,6,2 in the first round again.

TABLE III

Trace of an AIDA algorithm execution

The option of n1, n3, 5 and 6 in the second round respectively at the time n2 and n4 choose 0 they already have indices assigned at the point. The final result of AIDA s_1 = 3 at node n1, s2 = 2, for node n3, s3 = 4, and for node n3 s4=1 and for node n4.

5. CONCLUSION

Every algorithm as of now implemented has their own advantages, in this paper we are introducing Newton identity greatly decrease communication overhead. This can allow use of large number of slots consequently reduce the requirement of number of iterations. The solution of polynomial can be removed at one expense by using strum theorem. By using this technique we can provide security for anonymous persons by using ID sharing. In this some persons may give their information to public to share anyone. Here we are taken ID sharing concept to share the data in the group.

REFERENCES

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

[2] White Paper—The EssentialGuide toWeb AnalyticsVendor Selection, IBM [Online]. Available: http://measure.coremetrics.com/corem/getform/ reg/wp-evaluation-guide

[3] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

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

[5] 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.

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

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

[8] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game," in *Proc. 19th Ann. ACM Conf. Theory of Computing*, Jan. 1987, pp. 218–229, ACM Press.

AUTHOR PROFILE

V. Lasya pursuing M.Tech(CSE) from Sri Sunflower Engineering & Technology challapalli, krishna Dist Andhra Pradesh , Affiliated to JNTU-KAKINADA.

M. Prasanthi (M.Tech), working as Assistant Professor at Sri Sunflower Engineering & Technology challapalli, krishna Dist Andhra Pradesh , Affiliated to JNTU-KAKINADA.

Abdul Vahed (M.Tech, MISTE) , working as Associate Professor & HOD(CSE) at Sri Sunflower Engineering & Technology challapalli, krishna Dist Andhra Pradesh , Affiliated to JNTU-KAKINADA.