View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by International Institute for Science, Technology and Education (IISTE): E-Journals

Innovative Systems Design and Engineering
ISSN 2222-1727 (Paper) ISSN 2222-2871 (Online)
Vol.6, No.3, 2015
www.iiste.org

Emendation of Undesirable Attack on Multiparty Data Sharing With Anonymous Id Assignment Using AIDA Algorithm

Rene Thomas

Student, Department of CSE, Mar Baselios Christian College of Engineering and Technology, Kerala, India

Abstract

Security is a state of being free from danger or threat. When someone finds the vulnerabilities and loopholes in a system without permission means the system lacks its security. Wherever a secure data sharing occurs between multiparty there would be the possibility for undesirable attacks. In a variety of application domains such as patient medical records, military applications, social networking, electronic voting, business and personal applications there is a great significance of anonymity. Using this system we can store our data as groups and also encrypt it with encryption key. Only the privileged person can see the data. 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. Another algorithm for sharing simple integer data on top of secure sum is built. The sharing algorithm will be used at each iteration of this algorithm for anonymous ID assignment (AIDA). By this algorithm and certain security measures it is possible to have a system which is free from undesirable attacks.

Keywords: Vulnerability, anonymity, encryption key, secure multiparty computation, AIDA

1. Introduction

Nowadays security in multiparty data sharing is one of the most inevitable element. The emendation of undesirable attacks with AIDA algorithm and privacy preserving communications etc. are based on an assumption that each party is semi-honest. Internet involves and enables sharing of data but identity of the shared data owner is to be preserved. This is called maintaining anonymity that is quite difficult with increasing server storages like cloud, a problem area. Researchers have also investigated the relevance of anonymity and/or privacy in various application domains: patient medical records [1], electronic voting [2], e-mail [3], social networking [4], etc.

Defining privacy-preserving data access turns out to be harder than you might expect, because many superficially attractive definitions break down. Some definitions work if the analyst can ask only one question, but get into trouble if the analyst can ask multiple questions the analyst might be able to ask two harmless questions whose answers, taken together, reveal everything about an individual. Some definitions break down if the analyst has any access to outside information about the world, even basic information like the fact that the average human is less than ten feet tall. Some definitions turn out to be impossible to achieve in this universe. Differential privacy avoids all of these pitfalls.

The core of the definition is simple but subtle. Imagine two data sets, A and B, which are exactly identical except that A includes information about one additional person who is not included in B. Now we ask: If we let the analyst get answers to questions about our data set, can the analyst tell whether we are using data set A or data set B? If the analyst can't tell the difference and this result holds no matter which data set A we started with and no matter which person we excluded from B, then we have succeeded in preserving privacy. Why? Because any inference the analyst makes about you will have to be the same inference he would have made even if your information were not in the data set at all. To put it another way, including your information in the data set did nothing to harm your privacy. So whatever may be the things security is essential without the any default.

The main algorithm is based on a method for anonymously sharing simple data and results in methods for efficient sharing of complex data. a. There are many applications that require dynamic unique IDs for network nodes [5]. The IDs are needed in networks for security or for administrative tasks requiring reliability, such as configuration and monitoring of individual nodes, and download of binary code or data aggregation descriptions to these nodes. It further explores the connection between sharing secrets in an anonymous manner, distributed secure computation and random ID assignment. The network is not anonymous and the participants are identifiable in that they are known to and can be addressed by the others. This paper builds an algorithm for sharing simple integer data on top of secure sum.

2. Multiparty data sharing system

The existing system has many advantages and disadvantages. Existing and new algorithms for assigning anonymous IDs are examined with respect to trade-offs between communication and computational requirements. Also, suppose that access to the database is strictly controlled, because data are used for certain experiments that need to be maintained confidential. Clearly, allowing one person to directly read the contents of the tuple breaks the privacy of another; on the other hand, the confidentiality of the database managed by first is violated once second has access to the contents of the database. Thus, the problem is to check whether the database inserted with the tuple is still k-anonymous, without letting one's and second know the contents of the tuple and the database respectively. The current system has certain algorithms the secure sum allows us to share simple data anonymously even if it does not have enough security measures we are adding the anonymous data sharing power sums algorithm and finally we got a system which can send complex data but as it names signifies itself it is difficult to find the ways in which how it is arranged and further modification are also not possible. For the convenience of the system we are adding AIDA algorithm it is easy to send complex data but the data are not all secure and even a hacker can easily read the data and a cracker can easily change the contents.

Consider, group of hospitals (or any system which you want to share details) desire to share the average of data items by means of individual databases. Nodes contain data items and workout and allocate only the total value. Along with some assurances of anonymity, a secure sum algorithm permits the sum to be collected. To allocate the nodes identifiers, numbers ranging from 1 to N, was applied in the technique and the identities received are unidentified to the other members of the group and in that this assignment is anonymous. The semi-honest model of privacy preserving data mining was assumed, in which each node will go after the rules of the protocol, however may possibly use the information it spots during the implementation of the protocol to compromise security.To solve this problem, we use the secure um algorithm which is as follows:

Algorithm 1:Secure Sum [6][7]

Given nodes $n_1,\ldots,n_N$ each holding an data item d*i* from a finitely representable abelian group, share the value $T=\sum d_i$ among the nodes without revealing the values d_i.

Each node n_i, i=1,..,N chooses random values $r_{i,1},\ldots,r_{i,N}$such that

$r_{i,1} + \ldots\ldots + r_{i,N} = d_i$

1) Each "random" value $r_{i,j}$ is transmitted from node n_i to node n_j. The sum of all these random numbers $r_{i,j}$ is, of course, the desired total T.
2) Each node $n_j$totals all the random values received as:
   $s_j = r_{1,j} + \ldots + r_{N,j}$
3) Now each node $n_i$simply broadcasts s_i to all other nodes so that eachnode can compute:
   $T = s_1 + \ldots + s_N$

Algorithm 2: Anonymous Data Sharing With Power Sum [6]

Given nodes $n_1 \ldots n_N$ each holding a data item d_i from a finitely representable field , make their data items public to all nodes without revealing their sources.

1) Each node n_i computes d_i^n over the field F for n=1,2,….N . The nodes then use secure sum to share knowledge of the power sums:

$P_1 = \sum_{i=1}^{N} d_i^1$	$P_1 = \sum_{i=1}^{N} d_i^2$	⋯	$P_N = \sum_{i=1}^{N} d_i^N$

2) The power sums $P_1 \ldots P_N$ are used to generate a polynomial which has $d_1 \ldots d_N$ as its roots using Newton's Identities as developed. Representing the Newton polynomial as :

$p(x) = c_N x^N + \ldots + c_1 x + c_0 \quad (1)$

The values $c_0 \ldots c_N$ are obtained from the equations:

$C_N = -1$
$C_N - 1 = -1/1(C_N P1)$
$C_N - 2 = -1/2(C_N - 1P1 + C_N P2)$

C_N-3 = -1/2(C_N-2P1 +C_N-1P2+ $C_N P$3)……

$$C_N\text{-}m = -1/m \sum_{k=1}^{m} C_{N-m+k} Pk \qquad (2)$$

3) The polynomial p(x) is solved by each node, or by a computation distributed among the nodes, to determine the roots $d_1 \ldots d_N$.

The power sums P_i can be collected and shared using a single round of secure sum by sending them as an array and applying the method to the vectors transmitted and received. The power sums are symmetric functions, and thus no association is made between n_i and the value of d_i. However, nonetheless, the information contained in these sums can be used to find the values of the data items $d_1 \ldots d_N$ .The choice c_N= -1 may be replaced by c_N= 1 or any other nonzero value. Also, note that in the typical F=GF(P) case, the solution for the c_i requires finding the multiplicative inverse of the coefficients 2,3,..N modulo P. While the Euclidean algorithm could be used, the inverses 1/x can easily be computed in the order x=1,2…N by the formulae:

$$q = P/x + r; \quad 1/x = -q\,(1/r) \pmod{P}$$

After the integer division with remainder r, 1/r will already be known, since r< x.

Algorithm 3: Find AIDA [6]

Given nodes $n_1..n_n$, 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 n_i chooses a random number r_i in the range 1 to S. A node assigned in a previous round chooses r_i=0.

3) The random numbers are shared anonymously. One method for doing this was given. Denote the shared values by $q_1 \ldots q_N$.

4) Let $q_1 \ldots q_k$ 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 n_i which drew unique random numbers then determine their index s_i from the position of the random number in the revised list as it would appear after being sorted:

s_i= A+ card{ q_j: q_j<= r_i}

5) Update the number of nodes assigned : A =A+k;.

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

Each algorithm compared can be reasonably implemented and each has its advantages. Our 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 byusing Sturm's theorem. All of the non-cryptographic algorithms have been extensively simulated, and we can say that 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.

3. Enhanced System

The system using AIDA algorithm, it is easy to transfer complex data anonymously without any interference. For this we are having an admin or someone who can add the members and those want to participate in the data sharing. The system mainly deals with the efficient algorithms for assigning identifiers (IDs) [6] to the nodes of a network in such a way that the IDs are anonymous using a distributed computation with no central authority.

The Fig 1 of ideal system builds an algorithm for sharing simple integer data on top of secure sum. The sharing algorithm will be used at each iteration of the algorithm for anonymous ID assignment (AIDA). This AIDA algorithm, and the variants that we discuss, can require a variable and unbounded number of iterations. With the help of this system explores the connection between sharing secrets in an anonymous manner, distributed secure multiparty computation and anonymous ID assignment.

Fig. 1 Ideal System

The use of the term "anonymous" means the external data authentication purposes in real v/s ideal system in Fig 2 differs from its meaning in research dealing with symmetry breaking and leader election in anonymous networks.

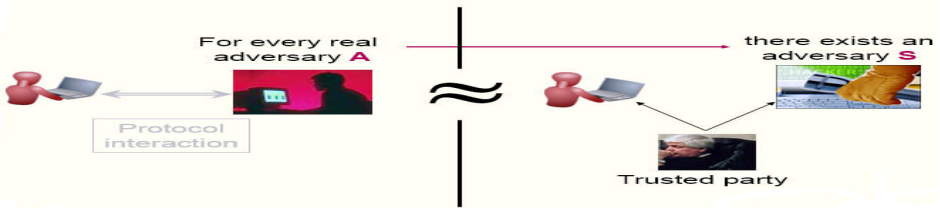

Fig 2 Real V/S Ideal Systems

Our network is not anonymous and the participants are identifiable in that they are known to and can be addressed by the others. Methods for assigning and using sets of pseudonyms have been developed for anonymous communication in mobile networks. The methods developed in these works generally require a trusted administrator, as written, and their end products generally differ from ours in form and/or in statistical properties.

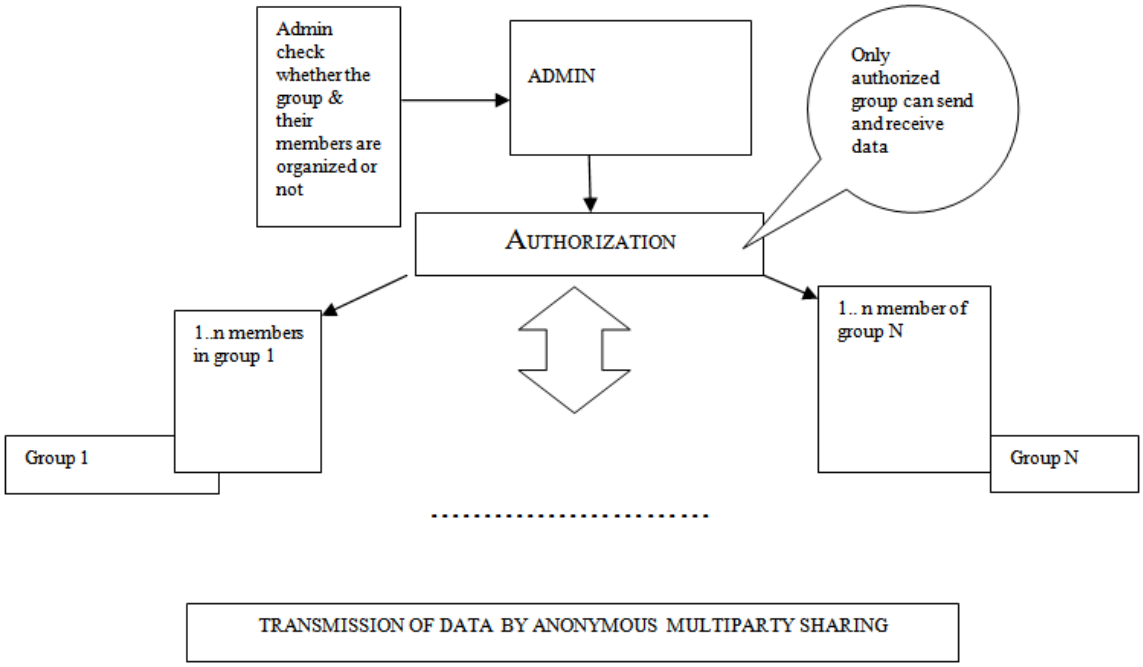

Fig 3. Architecture of data sharing

Fig 3 explains that increasing a parameter in the algorithm will reduce the number of expected rounds.Every members have anonymous id and they are known to the trusted third party. Suppose trusted third party say T, and admin say Main (M). If the group A need to send information to some members in 'i' groups. Each group have separate authentication, where the admin whether the group's authorized or not. Just like an authorization module for checking the password invalid or not. If it is an authorized group the One Time Password (OTP) will be generated and that generate did will be given to the group which we need to send, if these groups are also authorized. Then they were able to send information between them.After accessing the group id using OTP the message code will be generated. Then these message code will reached their appropriate destination. So that the message received by each member will be transferring required data as far as possible. Since each of the group can be send message only if they are authorized and for receiving message also it would be an authorized group. This is how the proposed system improves its security.

Simultaneously the messages will received by multiple members. Even though every members in the group does not need the entire information the id will provide the appropriate message if those id's are matching. This is how the anonymous id generated and adding some additional security measures and all the undesirable attacks in the multiparty data sharing with AIDA algorithmwill be possible.

4. Conclusion

The proposed system AIDA rule is the main thing in allocating ID to users and therefore the anonymous identity is maintained within the user and therefore the information owner isn't compromised below any circumstances therefore providing ample proof for the sets of users in multiparty environments. The anonymous identity is maintained in the user. The data owner is not compromised under any circumstances. Even under difficult situations the communications and bandwidth is not affected in any manner. AIDA proves to be secure for distributed architecture keeping the user safe from prying persons under attack 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. It is sure that an intruder can never enter into the system unless or until with help of centralized authority and then the message will send to all of the users who participating in this data sharing. Also mobile web services are an area of interest for future extensions to AIDA.Using this system we can ensure high security in all its aspects and many future enhancements can be done with the help of it.

REFERENCES

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

[2] 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.

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

[4] 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.

[5] J. Smith, "Distributing identity [symmetry breaking distributed access protocols]," *IEEE Robot. Autom. Mag.*, vol. 6, no. 1, pp. 49–56, Mar. 1999

[6] Larry A. Dunning, *Member, IEEE*, and Ray Kresman "Privacy Preserving Data Sharing With Anonymous ID Assignment" in IEEE transaction on information and forensics and security, vol 8, no. 2 february 2013

[7] Benjamin C.M. Fung, Member, IEEE, Thomas Trojer, Member, IEEE, Patrick C.K. Hung, Member, IEEE, Li Xiong, Member, IEEE,
Khalil Al-Hussaeni, Member, IEEE, and RachidaDssouli, Member, IEEE, "Service-Oriented Architecture for High-Dimensional Private Data Mashup" IEEE transactions on services computing,vol. 5, no. 3, july-september 2012

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