International Journal of Science Engineering and Advance Technology, IJSEAT, Vol 2, Issue 12, December - 2014 | ISSN 2321-6905

International Journal of Science Engineering and Advance Technology

An Algorithm Of Anonymous Id Assignment For Secure Data Sharing On A Network

Morampudi Satya Harish[1], Dr A. Rama Murthy[2],K.T.V Subbarao[3]
1 2 3 Department of Computer Science And Engineering
1 2 3 Akula Sree Ramulu institute of Engineering and Technology, prathipadu,Tadepalligudem,A.P,India
[1]Email- msatyaharish3@gmail.com,[2]Email- ram111_sai@yahoo.com, [3] Email- ogidi@rediffmail.com

Abstract:
Existing and new algorithms for assigning anonymous IDs are scrutinized with respect to trade-offs among communication and computational requirements. An algorithm for distributed solution of certain polynomials over limited fields improves the scalability of the algorithms. Another form of anonymity as used in secure multiparty computation allows multiple parties on a network to together carry out a global computation that depends on data from each party while the data supposed by each party remains unknown to the other parties. The new algorithms are constructed on top of a secure sum data mining operation using Newton's identities and Sturm's theorem. An algorithm for distributed solution of convinced polynomials over limited fields improves the scalability of the algorithms. Markov chain representations are used to find statistics on the number of iterations required and computer algebra gives closed form results for the completion rates.

Keywords: Anonymization and deanonymization, cloud and distributed computing systems, multiparty computation, privacy preserving data mining, privacy protection, security and trust in cooperative communications.

Introduction:
To distinguish anonymous ID assignment from anonymous communication believes circumstances where parties desire to show their data collectively but anonymously in slots on a third party site. The IDs can be used to allocate the slots to users while anonymous communication can let the parties to hide their identities from the third party. In another application it is probable to use safe sum to allow one to opt-out of a computation beforehand on the basis of sure rules in statistical disclosure limitation or throughout a computation and still to do so in an anonymous manner. Though very little is known with respect to methods allowing organizations to opt-out of a secure computation based on the results of the examination should they sense that those results are too educational about their data. An algorithm for anonymous sharing of private data among parties is developed. This technique is used iteratively to allocate these nodes ID numbers. This assignment is anonymous in that the identities received are unknown to the other members of the group. Confrontation to collusion among other members is established in an information theoretic intelligence when private communication channels are used. This assignment of serial numbers allows more compound data to be shared and has applications to other problems in privacy preserving data mining collision avoidance in communications and distributed database access. The required computations are dispersed without using a confidential central influence**.**

Related Work:
In looking for to state the security and privacy provided by our algorithms we are certainly providential to have a profusion of definitions to choose even when restricting ourselves with the semi-honest assumption. The option of definition should be dependent on considerations such as whether confidential or cryptographically tenable communications channels are used etc. We pursue the proposal of a reviewer that an exacting information theoretic definition of privacy be used. The central arguments of the proofs should stay useful when assessing the algorithms with respect to other models of secure multiparty computation. The use of the term "anonymous" here fluctuates from its meaning in research dealing with symmetry breaking and leader election in anonymous networks. Our network is not anonymous and the participants are individual in that they are known to and can be addressed by the others.

Existing Method:
A secure computation purpose extensively used to secure sum that allows parties to calculate the sum of their individual inputs without revealing the inputs to one another. This function is popular in data mining applications and also helps characterize the complexities of the secure multiparty computation. A cryptographic approach that could assurance finitely bounded termination even without a trusted authority.

Note that some mental poker algorithms could also be used to make this guarantee.

Disadvantages:

The algorithms for mental poker are more complex and utilize cryptographic methods. We assume that the participants are semi-honest also known as passive or honest-but-curious and carry out their required protocols loyally.

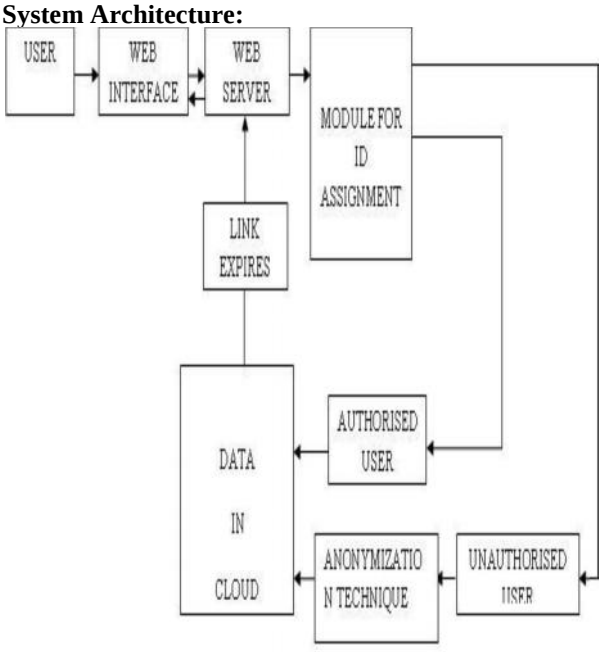
Proposed Method:

The proposed method deals with competent algorithms for assigning identifiers (IDs) to the nodes of a network in such a way that the IDs are unidentified using a distributed computation with no central authority. The main algorithm is based on a method for anonymously sharing easy data and results in methods for proficient sharing of complex data. The sharing algorithm will be used at each iteration of the algorithm for anonymous ID assignment (AIDA).

Advantages:

Increasing a parameter in the algorithm will reduce the number of expected rounds. That task limits the level to which it can be practically raised.

System Architecture:



Homomorphic Encryption Module:

To attain such goal the parties secure their messages by encrypting them. In order to carry out the privacy-preserving authentication of the database anonymity upon the insertion the parties use a commutative and homomorphic encryption method. This is designed at suppression-based anonymous databases and it permits the owner of DB to properly anonymize the tuple t without gaining any useful knowledge on its contents and without having to send to t's owner newly generated data.

Generalization Module:

The second protocol is aimed at generalization-based anonymous databases and it relies on a secure set intersection protocol such as the one found in to support privacy-preserving updates on a generalization based k-anonymous DB.

Cryptography Module:

A cipher or cypher is a pair of algorithms that produce the encryption and the reversing decryption. The detailed process of a cipher is controlled both by the algorithm and in each case by a key. This is a secret limitation ideally known only to the communicants for a specific message exchange context. The procedure of converting ordinary information called plaintext into incomprehensible gibberish called cipher text will be done in this type of module. Decryption is the reverse in other words moving from the unintelligible cipher text back to plaintext.

User And Admin Module:

The admin to encrypt the patient reports using encryption techniques using suppression and generalization protocols. To assemble the database based on the patient and doctor details and records in the respective protocol.

Algorithm Used:

Top-Down Refinement Algorithm

- Initialise completely masked table (one row, topmost values)
- Initialise list of possible refinements
- While some refinement is valid and beneficial
- Find best refinement
- Apply refinement and update list of possible refinements
- For all remaining refinements: update scores and validity
- End while
- Return masked T and set of refinements used
- For all remaining refinements: update scores and validity

■ Computation of entropy (InfoGain) needs to iterate over individual records

■ Computation of anonymity needs to count the „number of records"in each masked table.

Determining the „best refinement"

■ Refinement increases information gain, but decreases anonymity

■ Calculate trade-off score

■ Choose best refinement by maximum trade-off

Enhancement:

- Top-down refinement masks a given table to satisfy broad range of anonymity requirements

without sacrificing significantly the usefulness to classification.

- Top-down Refinement is much more efficient than previously reported approaches, particularly the genetic algorithm.

Conclusion:

Anonymity method presents privacy protection and usability of data. These schemes will safe secret sharing of private data by anonymous ID assignment. It is important that every cloud user must be certain that his data is stored, processed, accessed and audited in a tenable manner at any time. Getting done all these would come to an end up in attaining the long dreamt vision of secured Cloud Computing in the nearby future. Deal with efficient algorithms for assigning identifiers (IDs) to the nodes of a network in such a way that the IDs are anonymous.

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.

[9] A. Yao, "Protocols for secure computations," in *Proc. 23rd Ann. IEEE Symp. Foundations of Computer Science*, 1982, pp. 160–164, IEEE Computer Society.

[10] 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.

[11] 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.

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

[13] D. Jana, A. Chaudhuri, and B. B. Bhaumik, "Privacy and anonymity protection in computational grid services," *Int. J. Comput. Sci. Applicat.*, vol. 6, no. 1, pp. 98–107, Jan. 2009.

[14] D. M. Goldschlag,M. G. Reed, and P. F. Syverson, "Hiding routing information," in *Proc. Information Hiding*, 1996, pp. 137–150, Springer-Verlag.

[15] L.Willenborg and T.Waal, *Elements of Statistical Disclosure Control*, ser. Lecture Notes in Statistics. New York: Springer, 2001, vol. 155.

Authors:

Mr. Morampudi Satya Harish is a student of Akula Sree Ramulu institute of Engineering & Technology, Tadepalligudem. Presently he is pursuing his M.Tech [Computer Science and Engineering] from this college and he received his B.Tech from Eluru College of Engineering and Technology, affiliated to JNT University, Kakinada in the year 2012. His area of interest includes Computer Networks and Object oriented Programming languages, all current trends and techniques in Computer Science.

DR.A.RAMAMURTHY is Well Known Professor and he Received Ph.D from Jntu University and working as a Principal of Akula Sree Ramulu Institutions. He has 12 years of experience in various engineering colleges. His area of interest includes Object Oriented Programming Languages, Software Engineering, Operating Systems, Computer Networks and other advances in Computer Languages.

Prof. K.T.V Subbarao, well known Author and teacher received M.Tech (CSE) and working as Principal, Akula SreeRamulu institute of Engineering and Technology, He is an active member of ISTE. He has 12 years of teaching experience in various engineering colleges. To his credit couple of publications both national and international conferences/journals. His area of interest includes cryptography and network security, Distributed databases, Operating systems and other advances in computer Applications.