ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

DISTRIBUTED DATABASE R_K-SECURE SUM PROTOCOL

Jyotirmayee Rautaray[1], Raghvendra Kumar[2]

School of Computer Engineering, KIIT University, Odisha, India[1]

School of Computer Engineering, KIIT University, Odisha, India[2]

Abstract: Secure sum protocol of confidential data inputs is an exciting instance of Secure Multiparty Computation Protocol, which has attracted many researchers to devise secure protocols with highest privacy and lower probability of data leakage. In this paper, we proposed a protocol to compute the sum of individual data inputs with zero probability of data leakage when two neighbour parties join together to know the data of a center party. We break the data block of each party into number of data segments and redistribute the data segments among parties before the computation after adding the own random number. These complete steps create circumstances in which it becomes impractical for semi honest parties to know the private data of some other party presents in the Bus network architecture. In this all parties arranged in Bus topology. So the number of complexity of this protocol is decreased with zero percentage of data leakage. In this paper we proposed a distributed database Rk secure sum protocol.

Keywords: - Secure sum protocol, Secure multi party computation protocol, Privacy, Trusted third party, Without Trusted party, Information security

I. INTRODUCTION

The amount of growth of internet or network to compute some of the function by using different functional input without disclosing their own input to the other party. So this privacy plays an important role for calculating the common function. But for providing the privacy using different protocol for two party computations used e.g. Yao protocol [1], X ln (X) [1] [2] and secures sum protocol [1] [2] [5] [6] and for multi party computation protocol used secure multi party computation [3][11][12][13][14][15].

A. *Secure sum protocol*

Secure sum protocol [4] [5] [7] is used when two party want to compute the common function without disclosing their own input to the other party. In this protocol party P1 send the data block to another party presents in the network after adding the own random number. So that other party never able to know the other party result.

B. *Secure multi party computation protocol*

This protocol is applicable when the number of parties greater than or equal to two. In this protocol [6] [7] [8] [9] [10] one party is send its data segments after adding its own random number to the next party presents in the network. The secure sum computations model is divided into three models. One is homogeneous model, heterogeneous and another is hybrid model. In homogeneous model divided the database into number of horizontal partition database in row splitting manner so that other party will never the other party result this protocol is very useful in horizontal partition database. In heterogeneous secure sum model in which divide the database into vertical partitioning manner so that other party will never know the result of another party result.

C. *Trusted third party*

Trusted third model [8] [9] [10] [11] [12] [13] is also called ideal model. In which trusted third party play a impotent role to broadcast the global result, in this protocol all party will calculate their own result and send to the trusted third party then third party disclose the result.

D. *Without third party*

Without third party model [8] [9] [10] [11] [12] [13] is also called real model. In this model all parties calculate their result and one of the party broadcast the result to the rest of the party presents in the network.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

II. PROPOSED WORK

Let P1, P2… Pk are k parties concerned in mutual secure sum computation where each party is accomplished of breaking its data block into a fixed number of data segments [3] [5] [6] [7] [8] [9] such that the sum of all the data segments is equivalent to the value of the data block of that party. In proposed protocol quantity of data segments in a data block is kept equal to the number of parties [5]. The values of the segments are randomly selected by the party and it a secret of the party. If k be the number of segments (which is equal to the number of parties involved in the bus architecture) then in this protocol each party holds any one segment with it and k-1 data segments are sent to k-1 parties, one to each of the parties. Thus at the end of this rearrangement each of the parties holds k data segments in which only one data segment belongs to the party and other data segments belong to rest of parties presents in the network. In this proposed protocol, one of the parties is generally selected as the protocol initiator party which starts the computation by sending the data segment to the next party in the bus network. The receiving party adds its data segment and its secreted number and send to the next party presents in the architecture. This process is repeated until all the data segments of all the parties are added as well as data segments then the protocol initiator party is reduce the sum of all data segments then the sum is announced by the protocol initiator party. Now even if two adjacent parties maliciously cooperate to know the data of a middle party they will be able to know only those k data segments of a party which belong to every party. The sum of these data segments is a garbage value and thus worthless for the unauthorized parties. B1, B2 and B3 is a block of data then the segmentation break the block of data into the different number of data segments (D). Fig1 shows the distributed database Rk secure sum protocol before redistribution and fig2 shows the distributed database Rk secure sum protocol after the redistribution.

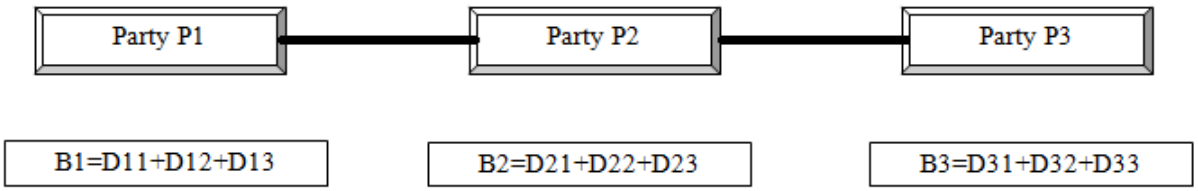

Fig1: Distributed database Rk secure sum protocol before redistribution of data segments

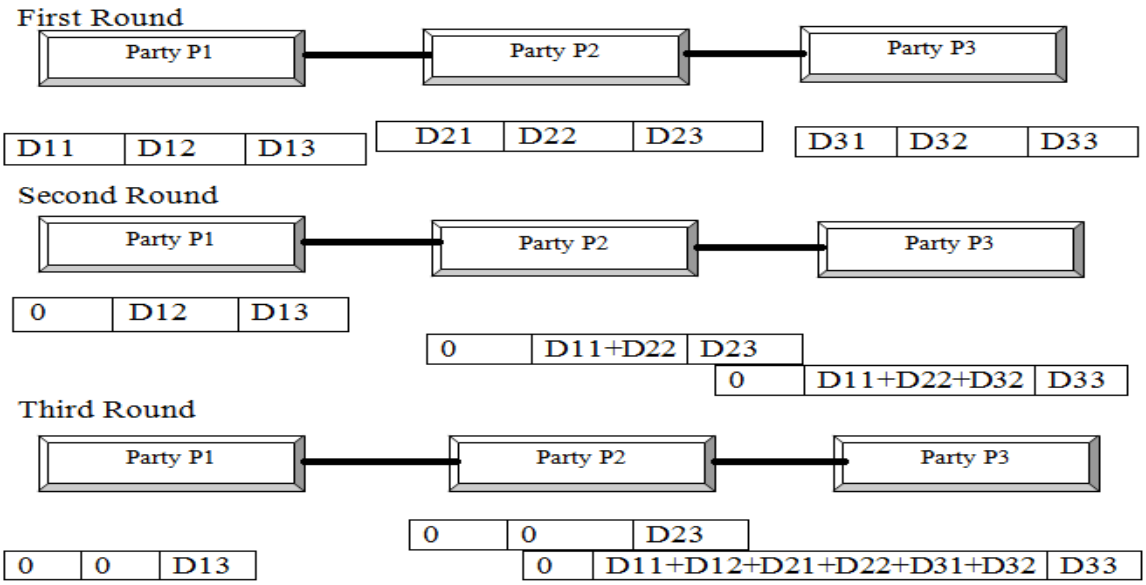

Fig2: Distributed database Rk secure sum protocol after redistribution of data segments

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

Algorithm: - Distributed database Rk secure sum protocol
Step1:- Select number of parties in bus network from P1, P2……..Pk /*where K=1 to N*/
Step2:- Select the random number from R1, R2…..Rk.
Step3:- Each party breaks the data block into different number of data segments Di1, Di2…….Dik/* where ∑Dik=Ri and J=1 to K*/
Step4:- Each party hold their only one data segments and distribute the rest of data segments after adding the random number to the rest of party presents in the bus network.
Step5:- After that each party rearrange the data segments and random number.
Step6:- Let Rc =K and Pij /*Rc Is round counter and Pij is Partial Sum where Pij= X. Support- minimum support*|size of the database| */
Step7:- While Rc! =0
Begin
For j=1 to K-1 do
For i=1 to K-1 do
Party Pi send the Pij=Dij + Rij to the Pk
Rc =Rc-1
End
Step8:- Party Pk broadcast the result to the rest of parties' presents in the bus network.
Step9:- End of process.

III. CONCLUSION

In this paper we proposed a Dk secure sum protocol for calculating the global result without disclosing the result of individual parties. For preserving privacy we used secure multi party computations with zero percentage of data leakage with high privacy. This protocol is advancements to all the previous protocol because this protocol is used bus topology to calculating the global result without disclosing their result. The number of this proposed protocol is N-1 so that the complexity of this protocol is in term of N its Θ (N).

REFERENCES

[1] A.C.Yao, "protocol for secure computations," in proceedings of the 23rd annual IEEE symposium on foundation of computer science, pp. 160-164, Nov.1982.
[2] C. Clifton, M. Kantarcioglu, J.Vaidya, X. Lin, and M. Y. Zhu, "Tools for Privacy-Preserving Distributed Data Mining," J.SIGKDD Explorations, Newsletter, vol.4, no.2, ACM Press, pp. 28-34, Dec. 2002.
[3] R. Sheikh, B. Kumar and D. K. Mishra, "Changing Neighbors k- Secure Sum Protocol for Secure Multi-party Computation," Accepted for publication in the International Journal of Computer Science and Information Security, USA, Vol.7 No.1, pp. 239-243, Jan. 2010.
[4] R. Sheikh, B. Kumar and D. K. Mishra, "Privacy-Preserving k- Secure Sum Protocol," in the International Journal of Computer Science and Information Security, USA, Vol. 6 No.2, pp. 184-188, Nov. 2009.
[5] R. Sheikh, B. Kumar and D. K. Mishra, "A Distributed k-Secure Sum Protocol for Secure Multi-party Computation," journal of computing, Vol.2 No.3, pp. 68-71, 2009.
[6] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game," in STOC '87: Proceedings of the nineteenth annual ACM conference on Theory of computing, New York, NY, USA : ACM, pp. 218-229, 1987.
[7] B.Chor and N.Gilbao. "Computationally Private Information Retrieval (Extended Abstract)," In proceedings of 29th annual ACM Symposium on Theory of Computing, El Paso, TX USA, May 1997.
[8] B. Chor, E. Kushilevitz, O. Goldreich,and M. Sudan, "Private Information Retrieval ," In proceedings of the 36th Annual IEEE Symposium on Foundations of Computer Science, Milwaukee WI, pp. 41-50, Oct. 1995.
[9] Y. Lindell and b. Pinkas, "Privacy preserving data mining," in advances in cryptography-Crypto2000, lecture notes in computer science, Vol. 1880, 2000.
[10] R. Agrawal and R. Srikant. "Privacy-Preserving Data Mining," In proceedings of the 2000 ACM SIGMOD on management of data, Dallas, TX USA, pp. 439-450, May 15-18 2000.
[11] M. J. Atallah and W. Du. "Secure Multiparty Computational Geometry," In proceedings of Seventh International Workshop on Algorithms and Data Structures(WADS2001). Providence, Rhode Island, USA, pp. 165-179, Aug. 8-10, 2001.
[12] W. Du and M.J. Atallah. "Privacy-Preserving Cooperative Scientific Computations," In 14th IEEE Computer Security Foundations Workshop, Nova Scotia, Canada, pp. 273-282, Jun. 11-13, 2001.
[13] W. Du and M.J.Atallah, "Privacy-Preserving Statistical Analysis,"In proceedings of the 17th Annual Computer Security Applications Conference, New Orleans, Louisiana, USA, pp. 102-110, Dec. 10-14 2001.
[14] W. Du and M.J. Atallah, "Secure Multiparty Computation Problems and Their Applications: A Review and Open Problems," In proceedings of new security paradigm workshop,Cloudcroft, New Maxico, USA, pp. 11-20, Sep. 11-13, 2001.
[15] V. Oleshchuk, and V. Zadorozhny, "Secure Multi-Party Computations and Privacy Preservation:Results and Open Problems,

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

BIOGRAPHY

Jyotirmayee Rautaray has received B. Tech. (Bachelor of Technology) degree in Computer Science and Engineering from Raajdhani Engineering College "BPUT University, Bhubaneswar (Odisha), India in 2011. She is Pursuing her M. Tech. (Master of Technology) in Computer Science from KIIT University, Bhubaneswar (Odisha), India in 2013. Her subjects of interest include Computer Networking, Theory of Computer Science, Data Mining, NLP and Analysis & Design of Algorithms. She has published 10 research papers in international journal. Her researches areas are Computer Networks, Data Mining, cloud computing, NLP and Secure Multiparty Computations.

Raghvendra Kumar has received B.Tech. (Bachelor of Technology) degree in Computer Science and Engineering from SRM University "Chennai" (Tamil Nadu), India in 2011. He is Pursuing his M.Tech. (Master of Technology) in Computer Science from KIIT University, Bhubaneswar (Odisha), India in 2013. His subjects of interest include Computer Networking, Theory of Computer Science, Data Mining and Analysis & Design of Algorithms. He has published 13 research papers in international journal and 5 papers in IEEE. His researches areas are Computer Networks, Data Mining, cloud computing and Secure Multiparty Computations.