ISSN: 2319-8753

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

Modified Distributed R_k Secure Sum Protocol

Jyotirmayee Rautaray[1], Raghvendra Kumar[2], Garima Bajpai[3]

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

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

School of Computer Engineering, KIIT University, Odisha, INDIA[3]

Abstract: Secure Multi-Party Computation allows various parties to compute several functions of their inputs with no disclosing the definite inputs to individual an added. Secure sum computation is an easily unwritten paradigm and the component of the different Secure Multi-Party Computation solutions. Secure sum computation allows parties to compute the sum of their individual inputs with no disclosing the inputs to one another. In this paper, we propose a modified version of Rk-Secure Sum protocol with additional security when a grouping of the computing parties conspires to know the data of some party.

Keywords: Privacy, Secure sum, Secure Multi Party computation, Modified Rk Secure sum protocol.

I. INTRODUCTION

The enormous growth of the Internet and its undemanding access by common man created opportunities for combined computations by numerous parties. All the participating parties for the sake of their joint benefit want to compute the ordinary function of their inputs but at the same time they are apprehensive about the privacy [6] [7] [8] [10] of their data. This subject of the information security is called Secure Multi- Party Computation. This subject has two goals; one is the privacy of the individual data inputs and another is the correctness of the result. Mainly two models are present in the journalism for the analysis of the Secure Multi-Party Computation problems. Ideal model of the Secure Multi-Party [11] [12] [13] [14] Computation uses a Trusted Third Party apart from the participating parties. Parties supply their inputs to the Trusted Third Party. Computation of the function is done by the Trusted Third Party and then the result is sent to all the parties. In this paradigm the trustworthiness of the Trusted Third Party is critically important because if the Trusted Third Party turns corrupt, it can supply the private inputs of one party to others. But it is extensively used model of the Secure Multi-Party Computation due to its easy implementation and the protocols available which prevent the Trusted Third Party to act maliciously. Real model of the Secure Multi-Party Computation does not use any Trusted Third Party but the parties themselves agree on some protocol for the computation. The party performance in the Secure Multi-Party Computation is important to reflect on. An honest party follows the protocol and respects the privacy of other parties. A semi honest party follows the protocol but also tries to learn other information than the result. The corrupt party neither follows the protocol nor respects the privacy of other parties. Different protocols are needed for dissimilar Secure Multi-Party Computation models and the behaviour of the party. Solutions are available for Secure Multi-Party Computation problems with Cryptographic techniques, Randomization techniques and Anonymization methods. The subject of Secure Multi-Party Computation has been evolved from two party relationship problems [1] to multi party representation pattern matching problems. Many specific Secure Multi-Party Computation problems have been defined and analysed by researchers approximating Private Information Retrieval, Selective Function Evaluation, Privacy-Preserving Database Query, Privacy-Preserving Geometric Computation, Privacy- Preserving Statistical Analysis, Privacy-Preserving Intrusion Detection and Privacy-Preserving Cooperative Scientific Computation. Based on these general Secure Multi-Party Computation problems many real life applications emerged like Privacy- Preserving Electronic Voting, Privacy-Preserving Bidding and Auctions, Privacy-Preserving Social Network Analysis, Privacy-Preserving Signature and Face Detection, etc. Secure sum computation problem of Secure Multi-Party Computation can be defined as: How multiple parties can compute the sum of their input values without disclosing definite values to one another. Secure sum can occupation as to implement for the Secure Multi-Party Computation solutions in the privacy preserving dispersed data mining problems [1] [2] [3]. We proposed novel Rk-secure sum protocols with more security in case a group of the parties join together and want to know the private data of some other party.

A. *Secure sum*

Secure sum [1] [4] [5] [6] is applicable only for two parties for providing the security. In this protocol one party send the partial support to the next party with adding their own random number then the last party will disclose the result. Many secure sum protocol are available like Yao (1), Ln(x) [2], secure union protocol etc.

ISSN: 2319-8753

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

B. *Secure Multi Party Computation*

Secure multi party computation (11) (14) (15) is applicable when the number of parties more than two. In which one party calculate their partial support and send to the next parties after adding the own random number. Then the last parties will disclose their result.

II. PROPOSED WORK

When the concept come of distributed database [8] [12] [13] in which the whole database is divided into the number of parties and each party want that their own result will not known by the other parties so concept of security and privacy play a important role. In this paper we proposed modified Rk Secure Sum protocol for providing the highest privacy to the distributed database. In this proposed protocol all the parties are arranged in a sequential manner and party P1 is consider as a protocol initiator party. If there are N numbers of parties then number of round is also N. But the condition is that party P1 will always changes their position in each round till the party Pn. And after that P1 will disclose the result. First the P1 calculate their own partial support and added their own random number and send to the next party till Pn. After the completion of N^{th} round party P1 will disclose the global result that accepted by all the parties presents in the distributed database. Algorithm shows formal working steps of modified Rk secure sum protocol. Fig 1 shows the number of rounds from 1, 2, 3, 4, and 5.

Algorithm of Modified Rk Secure sum Protocol

Step1:- Select N number of parties from P1, P2…….Pn. (N≥4).
Step2:- Consider each party has a random number R1, R2……..Rn.
Step3:- Arranged the parties in a bus structure and select P1 is protocol initiator.
*Step4:- Assume RC=n and Pij=0 /*RC is round counter and Pij is partial support */*
Step5:- While RC! =0
Begin for I=1 to n do
Each time Party P1 exchange its position till Pn
End
RC=RC-1
Step6:- Party P1 allowances the partial support (Pij).
Step7:- End of algorithm.

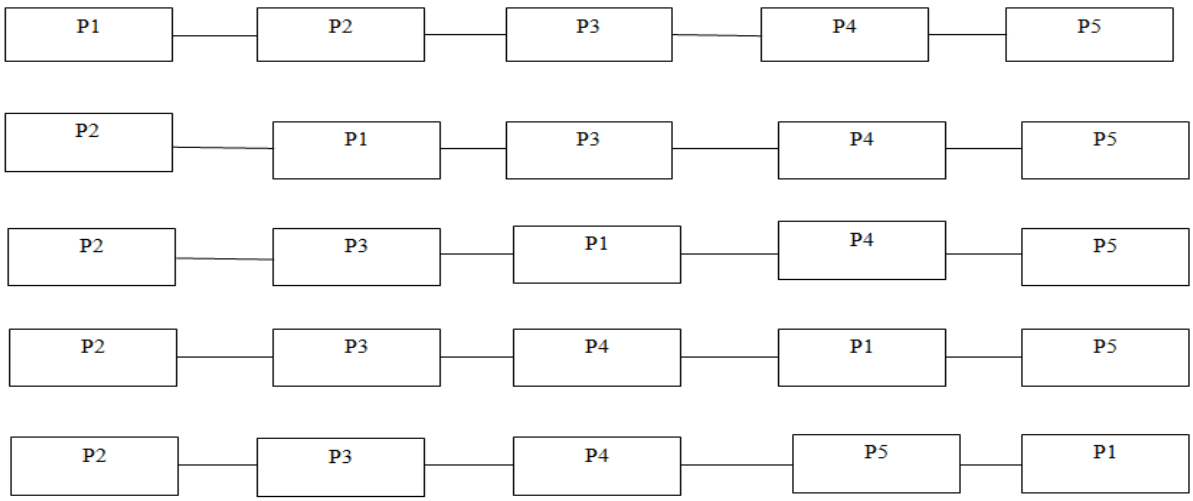

Fig 1: Shows the Process of each rounds (1, 2, 3, 4, 5)

III. CONCLUSION

Secure sum protocol is important concept of secure multi party computation. The secure multi party computation in which the probability of data leakage is Zero. In this proposed protocol provide zero percentage of data leakage is zero when two or more parties want to know the data for other nearer party. In this Modified Rk Secure sum protocol data is transferred in the form of blocks. So that the privacy required in this protocol is very less as compare to the segment of data transmission. The complexity of this protocol is O (N). And in future we will implement a protocol that have complexity less then O (N) and also provide the highest privacy to the distributed database.

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," *submitted to a journal*, 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,

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.

Garima Bajpai has received B. Tech. (Bachelor of Technology) degree in Computer Science and Engineering from Shri Rammurti Smarak college of Engineering and Technology "UPTU University, Barielly (Uttar Pradesh), India in 2009. 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 research papers in international journal. Her researches areas are Computer Networks, Data Mining, cloud computing, NLP and Secure Multiparty Computations.