ISSN: 2319-8753

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

STAR TOPOLOGICAL SECURE SUM PROTOCOL WITH TRUSTED THIRD PARTY

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 Multiparty Computation allows all parties to compute the common result of their individual data without disclosing their data to others party. Secure sum computation is one of the important tools of the Secure Multiparty Computation. In Secure Multiparty Computation lot of reputed researchers give their protocols, researchers show their interest. In this paper we proposed a new secure multi party computation protocol which is combination of both real and ideal model as well as the star topology for providing the highest privacy to the database with the zero percentage of data leakage and also the complexity of this protocol is very lesser as compare to other protocol and this protocol is useful for multi party computation. The complexity of this protocol is ϴ (n).

Keywords: secure sum, secure multi party computation, trusted third party, and star topology.

I. INTRODUCTION

Secure sum protocol [1] [2] [3] is applicable when the number of parties is only two not more than that. In this protocol the first party calculate their result and adds its key value (Random number) and send to the next party presents in the protocol for two parties. Cases the first protocol is used that is Yao protocol [1]. But if calculate the result when the number of parties greater than two then another protocol is used. That is secure multi party computation [2] [3] [4] [8] in which the number of parties greater than two. In this protocol each party calculate their result and add its key value and send to the next party presents in the network. This protocol is applicable for both real and ideal model. In real model there is no any existence of the trusted third party but in ideal model there is trusted third party play an important role for this protocol. Because the trusted third party broadcast the result to all the parties presents in the models. Star topological secure sum protocol is applicable for both real and ideal model as well as star topology in star topology [9] [10] [11] all the network is designed as star manner in which the main party presents in the middle of the network and all other party access the data from the center party so this protocol is very useful in case of trusted third party.

II. PROPOSED WORK

A In this proposed protocol star topological secure sum protocol [2] [3] [8] [9] [10] [11] each party divides the data blocks into number of data segments and each party selects their own random number for providing the high privacy to the database. So that other party never know the result of another party presents in this protocol. In this proposed protocol star topological secure sum protocol of secure Sum Computation is proposed as shown in figure 1. In star topological secure sum protocol third party and individual parties both do computation partially at their end. In this protocol each party divides its data in three different data segments and with each data segment parties add different random number. Fig 1 shows the star topological secure sum protocol.

Algorithm: - STAR TOPOLOGICAL SECURE SUM PROTOCOL

Step1: All party presents in the star topological secure sum protocol sends its sum of first segment D11, D21, D13,….Dn1 and random number R11, R21, R31…..Rn1 to trusted third party.
Step2:- Trusted Third party do sum of all the first segments received from all the parties P1, P2, P3….Pn i.e. Sum.
Step3:- Trusted Third party send sum Sum to party P1.
Step4:- Party Pi presents in star topological secure sum protocol subtracts its first random number Ri1 and adds its second data segment Di2 and its random number Ri2 and then send sum (sum) to next party Pi+1 presents in star topological secure sum protocol. These steps repeat till last party Pn.
Step5:-Last Party Pn send sum (sum (sum)) to previous party Pn-1.

Step6:- Previous Party Pn-1 subtracts its second random number Ri2 and adds its third data segment Di3 and its random number Ri3 and send sum to previous party Pi-1 presents in star topological secure sum protocol. This step repeat till Party Pi=Party P1
Step7:- Initial Party P1 send sum (sum (sum (sum))) to trusted third Party and Trusted third Party send this sum (sum (sum (sum))) to last party Pn.
Step8:- Last Party Pn subtracts its random number Rn2 and adds its third data segment Dn3 and send sum (sum (sum (sum (sum)))) to previous party Pn-1.
Step9:- Party Pi-1 subtracts its random number Ri3 and send sum (sum (sum (sum (sum)))) to previous party Pi-2. Repeat this step till party Pi=P1.
Step10:- Initial Party P1 sends sum (sum (sum (sum (sum)))) to trusted third party.
Step11:- trusted third party broadcast the sum (sum (sum (sum (sum)))) to P1, P2, P3,….Pn presents in star topological secure sum protocol.

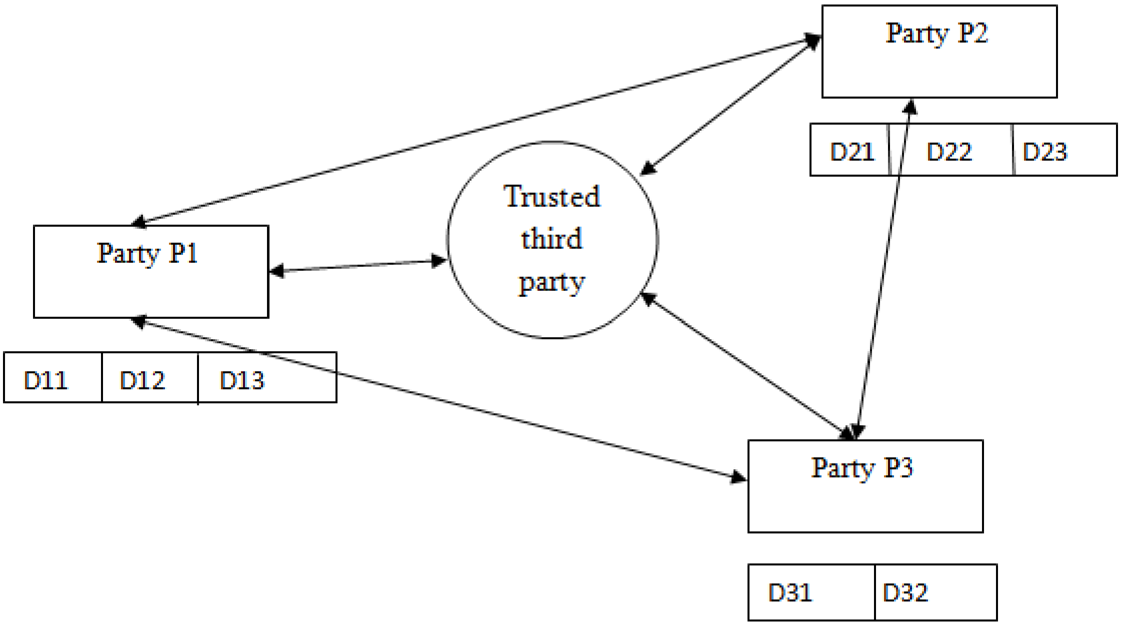

Fig 1 shows the star topological secure sum protocol

Star topological secure sum protocol is very useful because it's not dependent. if the trusted third party is malicious party then also it has not effect on this topological secure sum protocol because trusted third party only know the result of own and the data segments of the party to whom these are communicating as well as the party is malicious or hacker then that party only know their own result but not the other party result so it's very useful as compare to other protocol. And if all party present in Star topological secure sum protocol is honest party then the number of round is also decreases.
The complexity of this Star topological secure sum protocol after all steps is ϴ (n). Because at first step the trusted party start execution .so the number of step is 1 and second step is being processed through Party P1 to till party Pn. so the total number of step is n after that this process will continue in anti clock wise manner. So that same number of steps is n and after that all parties send the result to the trusted third party so that the number of step is only 1. That's why the total complexity is only ϴ (n) this very lesser as compare to other previous protocol.

III. CONCLUSION

In this paper we proposed a new secure sum protocol for secure sum computation. This model contains application of both ideal model and real model and this model used the star topology. so we named this protocol as a Star topological secure sum protocol.

In Star topological secure sum protocol computation of parties input data of individual parties is computed with the help of parties and trusted third party. Parties and trusted third party both do computation at their end and final result is broadcast by trusted third party to all the parties. This protocol gives data percentage of data leakage and also the highest privacy to individual party input data. And the complexity of this protocol is only in term of ϴ (n). So it's very lesser as compared to the other protocol. In future we propose a proposed protocol having the lesser complexity and highest privacy with zero percentage of data leakage.

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, 1982.

[2] Y. Lindell, “secure multiparty computation for privacy preserving data mining,” IBM, T.J. Watson Research Center, USA, http: // u.cs.biu.ac.il/-lindell/ research-statements / mpc- ppdm.htm/2001

[3] 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, 2001.

[4] O. Goldreich, S. Micali and A. Wigderson, “How to play any mental game.” In proceedings of the 19th annual ACM Symposium on Theory of Computation, pp218-229, 1987.

[5] Goldreich, “Multiparty Computation (Working Draft),” Available from http: //www.wisdom.weizmann.ac.il/ home / oded / public html / foc.html, 1998.

[6] 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, 2000.

[7] W. Du and M.J. Atallah. “Privacy-Preserving Cooperative Scientific Computations,” In 14th IEEE Computer Security Foundations Workshop, Nova Scotia, Canada, pp 273-282, 2001.

[8] W. Du and M.J. Atallah, “Protocols for Secure Remote Database Access with Approximate Matching,” In 7th ACM Conference on Computer and Communications Security (ACMCCS 2000), The first workshop on security and privacy in e-commerce, Athens, Greece, pp. 1-4, 2000.

[9] 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, 2001.

[10] W. Du and M.J.Atallah, “Privacy-Preserving Statistical Analysis,” In proceedings of the 17th Annual Computer Security ApplicationsConference, New Orleans, Louisiana, USA, pp.102-110, 2001.

[11] 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, 2002

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.